1963

Some structure theorems for p-groups

Edward A. Peressini
The University of Montana

SOME STRUCTURE THEOREMS FOR p-GROUPS

by

EDWARD PERESSINI

B.S. College of Great Falls, 1950

Presented in partial fulfillment of the requirements for the degree of Master of Arts.

MONTANA STATE UNIVERSITY

1963

Approved;

William R. Ballard
Chairman, Board of examiners

Frank C. Arbuckle
Dean, Graduate School

AUG 23 1963
Date

ACKNOWLEDGEMENTS

I take this opportunity to express my gratitutde to Professor William Ballard for his advice, guidance, and patience during the time this thesis was in preparation.

I wish to thank Professor Gloria Hewitt and Mrs. J. L. McDonald for their critical reading of the manuscript. Also I wish to dedicate this thesis to my wife, Lorraine, whose patience and understanding made this work possible.

TABLE OF CONTENTS

CONTENTS

TABLE OF NOTATION

$A, B, \ldots, G, H, \ldots$	groups or their subsets
$\|G\|$	order of G (cardinality)
$H \subseteq G$	H is contained in G
$\subset$	proper inclusion
$a \in G$	a is an element of G
$[G:H]$	index of H in G
G/H	factor group of G modulo H
$S = [a_\lambda]$	set of elements a_λ with λ ranging over some index set Λ.
$\{S\}$	subgroup generated by S
$O(a)$	order of element a
$m \mid n$	m divides n
$E(a)$	exponent of a
$H(x)$	height of x
nG	$\{nx \mid x \in G\}$
$G[p]$	$\{x \mid px = 0, x \in G\}$
I	the integers
$[a,b]$	lowest common multiple
$r(G)$	rank of G
$r_o(G)$	torsion-free rank of G
$r_p(G)$	p-rank of G
Λ, M	index sets of arbitrary power
(a,b)	greatest common divisor

INTRODUCTION

Groups may be classified as either abelian or non-abelian and, in either case, may be finite or countably or uncountably infinite. In turn, abelian groups may conveniently be classified as torsion groups, torsion-free groups, or of mixed character. This thesis is concerned chiefly with an investigation of certain structure problems encountered in the study of countable torsion groups. Our aim is to present complete systems of invariants; that is, sets of integers, cardinals, and ordinals which are characteristic of isomorphic groups but are different for non-isomorphic groups. The rank of a free abelian group and the set of orders of the cyclic direct summands of a finite group are examples of complete sets of invariants. Only torsion groups are considered since no complete sets of invariants have been found for the more general cases, except for a few special classes of groups.

An enormous effort has been expended on the study of groups, but until recently the research has been directed primarily toward finite groups. As a result of these studies, it is apparent that the strongest results are obtained when commutativity is assumed.

H. Prüfer, H. Ulm, and L. Zippin, in early investigations of the structure of abelian groups, produced im-

portant results in the theory of countable abelian groups without elements of infinite height. The theory of torsion-free abelian groups has been greatly enhanced by the works of R. Baier, A. Kurosh, and D. Derry, especially in the case of groups with finite rank. For mixed groups, the search for general structural results has been advanced by the papers of R. Baer. Although no complete structural results are yet known for groups of arbitrary order, two papers by L. Kulikov have stimulated penetrating research. A large variety of problems concerning abelian groups have been solved during the past decade leading to a wealth of interesting results, to a simpler theory, and to a clearer understanding of the underlying concepts involved.

To present the material more clearly, Chapter 0 is devoted to a collection of concepts and definitions of terms which are used more or less regularly throughout the thesis. In addition, other remarks, definitions, and concepts are introduced as they become necessary in the ensuing chapters. Included is a theorem which reduces the study of torsion groups to a study of the relatively simple primary group. The examples of groups cited include cyclic and quasicyclic groups to which we will refer many times.

Chapter I deals with the direct sum of cyclic groups. Here we consider free, finite, and finitely generated groups. Prüfer's Theorem, Theorem 1.9, the first of three essential results to be presented, is included.

This theorem describes the structure of countable primary groups. We also consider subgroups of direct sums of cyclic groups and other related topics.

Divisible groups are considered in Chapter II. The direct summand property, structure theorems on divisible groups, and the problem of embedding a given group in a divisible group are treated.

The structure problems encountered relative to absolute direct summands, pure subgroups, and factor groups with respect to pure subgroups are dealt with in Chapter III. In Chapter II, we conclude that a group is a direct summand of every group containing it if and only if it is divisible. As a point of interest we remark that a consideration of the analogous idea for pure subgroups, that is, the consideration of groups that are direct summands of every larger group in which they are contained as pure subgroups, leads to the topological concept of algebraic compactness as formalized by I. Kaplansky.

Basic subgroups are introduced and examined rather closely in Chapter IV. These subgroups are not only of independent interest, but are referred to again in Chapter V.

In Chapter V, we consider the two remaining essential structural results, the theorems of Ulm and Zippin. A large portion of this chapter is devoted to the construction of systems of invariants. We justify our choice of the theorems of Prüfer, Zippin, and Ulm as essential.

CHAPTER O

PRELIMINARY RESULTS AND DEFINITIONS

SECTION I

DEFINITIONS

At the outset, let us agree that the term "group" will always mean abelian group in the additive sense; that is, a non-empty set G of elements with a binary composition "+" such that

i) in the equation a + b = c any two of the elements a,b,c in G determine uniquely the third one;

ii) the associative law holds: (a + b) + c = a + (b + c) for all a,b, and c in G;

iii) the commutative law holds: a + b = b + a for all a and b in G.

We remark that postulate i) combines the closure law, the zero law, and the inverse law into a very compact statement. The associative law allows us to write the sum of two or more group elements without parentheses; the commutative law allows us to permute the terms of a sum.

1. Subgroups. A collection of elements H in a group G is said to form a subgroup of G if H forms a group with respect to the same binary composition defined on G. We list some of the more important facts concerning subgroups. For proofs of the statements, we refer the reader

to the list of references concluding this thesis, or in many cases, to any standard text in algebra.

1A) A set H in G is a subgroup of G if and only if when a and b are elements in H, then (a - b) is also an element in H.

1B) If H and K are subgroups of G then their intersection is again a subgroup of G. In fact, this particular property carries over for any number of subgroups.

1C) The set S of all elements a_λ, where λ ranges over some arbitrary set Λ will be denoted by $S = [a_\lambda]_{\lambda \in \Lambda}$. By $\{S\}$, we mean the subgroup generated by S; i.e., the intersection of all subgroups of G containing S. Thus, if S consists of the elements a_λ with λ in Λ, we write $\{S\} = \{\ldots, a_\lambda, \ldots\}$, and observe that $\{S\}$ consists of all finite linear combinations of the elements of S; i.e., all sums of the form $n_1a_1 + n_2a_2 + \ldots + n_ka_k$ where the n_i are integers, the a_i are elements of S, and k is any positive integer. In case $\{S\} = G$ we say that S is a generating system of G and that the elements of S are generators of G. A group G is called finitely generated if it possesses a finite generating system.

2. Cosets and index. If G is a group, H a subgroup of G, and a any element in G, then the set of elements a + h, h arbitrary in H, is called the coset generated by a and H. For example, let G be the set of all the vectors in Euclidean 2-space with the usual

conventions of equality, addition, and scalar multiplication. Let H be the set of all vectors with second component 0. Then a + H has as its geometric representation a line parallel to the axis of reals, through the point a. Recall that G is assumed to be commutative.

2A) If H is any subgroup of G, then every element of G belongs to some coset a + H.

2B) The sets H and a + H have the same number of elements.

2C) If two cosets a + H and b + H have one element in common, then they are identical. Thus two cosets are either identical or they are disjoint.

2D) The elements a and b of G belong to the same coset if and only if (a - b) is in H; this fact will be denoted $a \equiv b \bmod(H)$.

2E) If b is any element in a + H we may, by 2C), write a + H = b + H. In particular, if h is in H, then h + H = H.

2F) Suppose H, a + H, b + H, ... represent all of the different cosets of H in G, then G is the set-theoretic union of the pairwise disjoint sets.

2G) The index of H in G is the cardinal number of the set of different cosets of H in G. The index is denoted [G:H].

3. Factor groups. Let G be a group and H a subgroup of G. Then the set whose elements are the cosets

of H in G with the operation defined below is called the factor group of G by H; it will be denoted G/H.

3A) In G/H, addition is defined by using representatives: the sum of the two cosets a + H and b + H is the coset c + H consisting of elements of the form (a + h') + (b + h"), where a + h' is an element of a + H and b + h" is an element of b + H. The subgroup H acts as the identity element in G/H, and the inverse of the coset a + H in G/H is the coset (-a + H).

3B) There is a one-to-one correspondence between the subgroups of G/H and the subgroups of G which contain H.

4. Order. By the order of a group we mean the cardinal number of the set of its different elements. The order of G is denoted by |G|. G is a finite group if the order of G is a finite cardinal. A torsion group is a group in which every element has finite order; a group in which all non-zero elements have infinite order is called torsion-free. A mixed group has non-zero elements of finite order as well as elements of infinite order. By a primary-group or p-group, we mean a group in which the orders of the elements are powers of one and the same prime p.

4A) If G is a finite group and H is a subgroup of G, then |H| divides |G|.

4B) A finite group of prime order is cyclic.

5. Exponent and height. The next two concepts are defined for p-groups. If a is an element of order p^n; i.e., an element of a group G with the property that the subgroup $\{a\}$ generated by the element a has order p^n, we call n the exponent of a, and write $n = E(a)$. Let k be the greatest non-negative integer r for which $p^r x = a$ is solvable for some x in G, with a fixed a. This k is called the height $H(a)$ of a. If there is no such k; i.e., if $p^r x = a$ has a solution for every positive integer r, we say that a is of infinite height and set $H(a) = \infty$.

For any group G and any positive integer n, nG will denote the set of the elements of the form nx where x belongs to G. The set of all y in G satisfying $ny = 0$ is denoted G[n]. Writing O(a) for the order of an element a, we note that a is in nG if and only if $nx = a$ is solvable with respect to x and b is in G[n] if and only if O(b) divides n.

5A) In case G is a p-group, $H(a) = \infty$ is equivalent to the statement: $a \in p^n G$ for all positive integers n.

5B) If G is a p-group, the set G[p] is called the socle of the p-group G.

5C) If H(x) and H(y) are not equal, then H(x + y) is precisely the smaller of the two heights H(x) and H(y).

5D) If $H(x) = H(y)$, then $H(x + y) \geq H(x)$.

5E) $H(0) = \infty$. We remark that when we state that G has no elements of infinite order we mean no elements

other than the zero element.

6. Isomorphism. Two groups G and G' are called isomorphic if there exists a one-to-one correspondence $x \to x'$ of G onto G' such that $(x + y)' = x' + y'$; i.e., such that the operations in G and G' are preserved. If G is isomorphic to G', we write $G \cong G'$.

6A) Isomorphic groups are abstractly equivalent; they are indistinguishable except for symbolism.

6B) Any two cyclic groups of the same order are isomorphic.

6C) For all subgroups H and K of G we have $\{H,K\}/K \cong H/(H \cap K)$. Here $\{H,K\}$ means $\{H \cup K\}$.

6D) $G/H \cong (G/K)/(H/K)$ if H and K are subgroups of G such that $G \supseteq H \supseteq K$.

7. Homomorphism. If we drop the requirement that the mapping or correspondence be one-to-one we obtain a fundamental generalization of the concept of an isomorphism. A mapping η of a group G into a group G' is called s homomorphism if $(x + y)\eta = x\eta + y\eta$. If η is a homomorphism of G onto G', then G' is called a homomorphic image of G, symbolically $\eta : G \to G'$. A homomorphism of a group into itself is called an endomorphism; an isomorphism of a group onto itself is called an automorphism.

7A) The image $G\eta$ of a homomorphism of G into G' is a subgroup of G'.

7B) If η is a homomorphism of G into G', the inverse image $K = \eta^{-1}(0')$ of the identity of G' is a subgroup of G. The group K is called the kernel of the homomorphism.

7C) The fundamental theorem of homomorphisms for groups states that if G is a group and H is any subgroup of G, then the mapping ν: $a \to a + H$ of G onto G/H, the factor group of G by H, is a homomorphism. The mapping ν is called the natural homomorphism. If G' is a homomorphic image of G, then G' is isomorphic to a factor group of G.

8. Direct sums. Suppose A and B are two subgroups of a group G satisfying:

i) $\{A,B\} = G$ and

ii) $A \cap B = \{0\}$,

then G is called the direct sum of its subgroups A and B. We write $G = A + B$. For an arbitrary element g in G, i) allows us to write $g = a + b$ where $a \in A$, $b \in B$. By ii) we know that this representation is unique, for if $g = a + b$ and also $g = a' + b'$ with $a' \in A$ and $b' \in B$, then

$$a + b = a' + b', \text{ or } a - a' = b - b',$$

an element in $A \cap B = \{0\}$. A subgroup A of a group G is called a direct summand of G if there exists a subgroup B of G such that $G = A + B$. Then B is a complementary direct summand of A in G. The concept of a direct

sum may be generalized as follows: let A_λ ($\lambda \in \Lambda$) be a set of subgroups of G such that

i) $\{\ldots, A_\lambda, \ldots\} = G$; i.e., the A_λ together generate G, and

ii) for every $\lambda \in \Lambda$, $A_\lambda \cap \{\ldots, A_\mu, \ldots\} = \{0\}$ whenever μ ranges over all indices different from λ.

Then G is the direct sum of its subgroups A_λ, $G = \sum_{\lambda \in \Lambda} A_\lambda$. Any element $g \in G$ may be written in the form

$$g = a_1 + a_2 + \ldots + a_k$$

where each a_i comes from one of the sets A_λ and no two of the a_i come from the same A_λ. (It is understood that we are considering only non-zero a_i).

8A) If $G = A + B$, then $B \cong G/A$.

8B) If $g = a + b$ is an element of $G = A + B$ where $a \in A$ and $b \in B$, then $O(g) = [O(a), O(b)]$, the least common multiple of $O(a)$ and $O(b)$.

8C) Let $G = \sum_{\lambda \in \Lambda} A_\lambda$ and $G = \sum_{\mu \in M} B_\mu$ be two direct decompositions of the group G. These two decompositions are isomorphic if there exists a one-to-one correspondence between Λ and M such that corresponding components are isomorphic.

9. Linear independence and rank. The non-zero elements $a_1, a_2, \ldots, a_k$ of the group G are linearly independent if any relation

$$n_1 a_1 + n_2 a_2 + \ldots + n_k a_k = 0 \text{ with } n_1, n_2, \ldots, n_k$$

integers implies

$$n_1a_1 = n_2a_2 = \ldots = n_ka_k = 0.$$

We observe that in order that the requirement be satisfied if $O(a_i) = \infty$, then $n_i = 0$; if the order of an element is finite, $O(a_i) = m$, then m must divide n_i. A set of elements that is not independent is called dependent.

9A) If $L = [a_\lambda]_{\lambda\varepsilon\Lambda}$ is a set of elements of G where Λ is an index set of arbitrary power, then L is called independent if every finite subset of L is independent.

9B) A subset $[a_\lambda]_{\lambda\varepsilon\Lambda}$ of elements of G is independent if and only if the subgroup generated by the a_λ is the direct sum of the $\{a_\lambda\}$.

9C) An independent set M in G is called maximal if there is no independent set containing M properly. The maximality of M implies that any set [M,g] formed by annexing a non-zero element $g \varepsilon G$ to M is no longer independent and there exists a dependence relation

$$0 \neq ng = m_1x_1 + m_2x_2 + \ldots + m_kx_k$$

with $x_i \varepsilon M$ and $n, m_1, m_2, \ldots, m_k$ integers. In paragraph 10 we state the Axiom of Choice. The axiom enables us to extend any independent set to a maximal one. In fact, if the independent set contains only elements of infinite and/or prime power order, the extension may be accomplished using only elements of infinite and/or prime power order.

9D) For elements of finite order, an element $a \varepsilon G$ is said to be of smaller order than the element $b \varepsilon G$ if

$O(a) < O(b)$. We have need for a manner of distinguishing between elements of infinite order. Suppose $L = [a_\lambda]_{\lambda \in \Lambda}$ is some independent set of elements of G. Let a and b be elements in G with infinite order, with $a \in L$. Now if

$$rb = sa + s_1 a_1 + \ldots + s_k a_k \neq 0$$

with $a_i \in L$, $a_i \neq a$, r,s,s_i integers, and $s \neq 0$, then b is of <u>smaller order</u> than a relative to L, if $|r| < |s|$; b is of <u>greater order</u> than a, relative to L, if $|r| > |s|$.

9E) In the event that $G = \Sigma \{a_\lambda\}$, then $[a_\lambda]_{\lambda \in \Lambda}$ is called a basis of G. Thus a <u>basis</u> is a set $[a_\lambda]_{\lambda \in \Lambda}$ of elements of G such that G is the direct sum of the cyclic subgroups $\{a_\lambda\}$.

9F) The <u>rank</u> of a group G, denoted r(G), is defined to be the cardinal number of a maximal independent system in G containing only elements of infinite and/or prime power order. The symbol $r_o(G)$ denotes the <u>torsion-free</u> rank of G; it is the cardinal number of an independent set containing only elements of infinite order and being maximal with respect to this property. If G is a torsion group, then $r_o(G) = 0$. There is a similar definition for the <u>p-rank</u> of G, denoted $r_p(G)$, where elements whose orders are powers of the prime p are used in place of elements of infinite order.

10. <u>Axiom of Choice</u>. For any family F of non-void subsets $\{S_i\}$ of a set S, there is a choice function $f: F \to S$ such that $f(S_i) \in S_i$ for each i.

The Axiom of Well-Ordering, Zorn's Lemma, and Zermelo's Axiom are all logically equivalent to the Axiom of Choice. We include these three statements because virtually every theorem considered makes use of one of the forms, either explicitly or implicitly; in addition, they are of interest per se.

In an infinite group we cannot use finite induction on its order, and so some substitute is needed to replace this method of proof which is so valuable for finite groups. One way to make this replacement is to appeal to certain general axioms on sets and ordering. Suppose that we have an ordering relation $a \leq b$ on the elements of a set S of objects $\{a, b, c, \ldots\}$. The ordering may satisfy some of the following axioms:

O1) If $a \leq b$, and $b \leq a$, then $a = b$.

O2) If $a \leq b$, and $b \leq c$, then $a \leq c$.

O3) Either $a \leq b$ or $b \leq a$ for any two a,b.

O4) Any non-empty subset T of S has a first element x_1; i.e., an element x_1 such that $x_1 \leq t$ for every $t \in T$.

A set satisfying the first two axioms is called <u>partially ordered</u>. A <u>simply ordered</u> set or chain satisfies the first three axioms. If all four axioms hold, we say that the ordering is a <u>well-ordering</u>. We may appeal to the axiom of well-ordering: <u>Every set may be well-ordered</u>. We write $a < b$ to mean $a \leq b$ but $a \neq b$.

In a well-ordered set we may prove propositions by

transfinite induction. Let the first element of S be designated by 1. Then, if P(a) is a proposition about the elements of S and if P(1) is true, and if the truth of P(x) for all $x < a$ implies the truth of P(a), we conclude that P(b) is true for all $b \varepsilon S$. For let T be the subset of S, such that P(t) is false for $t \varepsilon T$. If T is non-empty, it contains a first element c. But then either $c = 1$ or P(x) is true for all $x < c$. In either event this would lead to the truth of P(c) contrary to the choice of c in T. Hence T must be empty and P(b) true for all $b \varepsilon S$. We note in passing that in a well-ordered set any descending sequence

$$a_1 > a_2 > a_3 > \ldots$$

is necessarily finite since it must contain a first element.

Zorn's Lemma. Given a partially ordered set S. Suppose that every simply ordered subset of S has an upper bound (lower bound) in S. Then S has a maximal (Minimal) element. Here if U is a subset of S, then an upper bound b of U is an element such that $b \geq u$ for all $u \varepsilon U$. A maximal element w has no upper bound different from itself. Reversing the inclusion, we similarly define lower bound and minimal element.

Suppose we consider subgroups of a group G partially ordered by inclusion: $A \subseteq B$ if A is a subgroup of B. Then the union of all elements in a simply ordered family of subgroups will itself form a subgroup. For this reason Zorn's Lemma is well suited to proofs in group theory.

Zermelo's Axiom. Zermelo proved that every set can be well-ordered if it is assumed that in each subset T of a set S one element of T can be chosen or designated as a special element. This assumption is precisely the Axiom of Choice and is equivalent to the assumption that, for any aggregate of pairwise non-intersecting sets, there is at least one set which has exactly one element in common with each of the sets of the aggregate.

SECTION 2

EXAMPLES

A) Cyclic Groups. A group G is a cyclic group if each of its elements is an integral multiple na of some fixed element a of G. A cyclic group G is denoted $G = \{a\}$. The order of the element a may be either finite or infinite. If all multiples of a are distinct; i.e., if $O(a) = \infty$, then the cyclic group is of infinite order and is isomorphic with the additive group of all integers under the mapping $\eta : na \to n$ with n, an integer. Therefore, all infinite cyclic groups are isomorphic; we denote these groups by the symbol $\mathcal{C}(\infty)$. The only generators of $\{a\}$ are a and -a. Consider a nonzero integer k different from +1 and -1. The cyclic group $D = \{ka\}$ is again a group $\mathcal{C}(\infty)$ with index k. The factor group $\{a\}/D$ can be generated by the coset $a^* = a + D$, and is of order k. We conclude that all proper factor groups of infinite cyclic groups are finite cyclic groups. If $\{a\}$ is cyclic of order m, then an element ka of $\{a\}$ is a generator of $\{a\}$ if and only if $(k,m) = 1$. If $O(a) = m$, then $\{a\}$ is isomorphic to the additive group of integers mod m, and we conclude that all finite cyclic groups of order m are isomorphic. These groups are denoted $\mathcal{C}(m)$. Subgroups of a finite cyclic group are again cyclic. In addition, the factor groups are also cyclic and possess the interesting

property that for subgroups D_1 and D_2 of $\{a\}$, $\{a\}/D_1 \cong \{a\}/D_2$ if and only if $D_1 = D_2$.

B). Complete and Discrete Direct Sum. Suppose we are given two groups A and B and are asked to find a group G which might be considered as the direct sum of A and B. Consider the set of all possible (ordered) pairs (a,b) with $a \in A$ and $b \in B$, subject to the rules:

i) $(a,b) = (a',b')$, with $a' \in A$, $b' \in B$, if and only if $a = a'$ and $b = b'$;

ii) $(a,b) + (a',b') = (a + a', b + b')$.

Then we obtain a group G of pairs (a,b) in which the elements (a,0) with $a \in A$, form a subgroup A' of G isomorphic to A under the mapping $\eta: (a,0) \leftrightarrow a$. Similarly, the elements in G of the form (0,b) constitute a subgroup B' of G isomorphic to the group B under the mapping $\emptyset$: $(0,b) \leftrightarrow b$. We may write $G = A' + B' = A + B$, because of the isomorphisms η and $\emptyset$.

We may generalize the preceding ideas to construct a group G which is the direct sum of any number of groups. Suppose we are given an indexed system of groups A_λ, where $\lambda \in \Lambda$. We wish to find a group G which is the direct sum of the A_λ ($\lambda \in \Lambda$). The elements of the Cartesian product of the A_λ ($\lambda \in \Lambda$) are the "vectors" obtained by taking as components one element from each of the groups A_λ. We further require that all but a finite number of the components must be zero. The set of all elements with an

element of A_λ in the λ-place and 0 in every other place constitute a group A'_λ which is isomorphic to the group A_λ under the mapping Ψ: $(0,..,0, a_\lambda, ...) \Leftrightarrow a_\lambda$. We then have $G = \sum_{\lambda \in \Lambda} A_\lambda$. The group G thus constructed is called the (discrete) direct sum of the A_λ. If all the A_λ are isomorphic to the same group A, then we denote the direct sum by $G = \sum_m A$ where m is the cardinal of the set of components.

If we omit the requirement that almost all components should vanish, then the group of vectors obtained is called the complete direct sum C of the A_λ. In this case we write $C = \sum_{\lambda \in \Lambda} A_\lambda$.

C) The Quasicyclic Group, $\mathcal{C}(p^\infty)$. Let p be a fixed prime and consider the p^kth complex roots of unity, k running over all the positive integers. They form an infinite multiplicative group; we shall use the additive notation in place of the multiplicative notation. This group, called a quasicyclic group, is denoted by $\mathcal{C}(p^\infty)$ and may also be described as follows. It is generated by elements $c_1, c_2, \ldots, c_n, \ldots$ such that

$$c_1 \neq 0,\ pc_1 = 0,\ pc_2 = c_1,\ \ldots,\ pc_{n+1} = c_n,\ \ldots.$$

Thus $O(c_n) = p^n$ and each element of $\mathcal{C}(p^\infty)$ may be written as a multiple of some c_n.

Let D be a proper subgroup of $\mathcal{C}(p^\infty)$. D cannot contain all the generators c_n; let c_{n+1} be the generator of smallest index which does not belong to D. Then $D = \{c_n\}$. To see this, we observe that $c_n \in D$ by our choice of c_{n+1}.

On the other hand, each $b \in D$ may be written in the form $b = kc_s$ for some k and s, and we may assume that k is not divisible by p. Then there are integers r, t with

$kr + p^s t = 1$, and we obtain

$$c_s = krc_s + p^s t c_s = rb \in D,\ s \leq n \text{ and } b \in \{c_n\},$$

establishing $D = \{c_n\}$. It follows that all proper subgroups of $\mathfrak{C}(p^\infty)$ are finite cyclic groups of order p^n $(n = 0,1,\ldots)$. These subgroups $\mathfrak{C}(p^n)$ of $\mathfrak{C}(p^\infty)$ form a chain with respect to inclusion; i.e., one of any two subgroups contains the other. For each n, there exists only one subgroup of order p^n; namely, that generated by c_n. All quasicyclic groups belonging to the same prime p are isomorphic.

$\mathfrak{C}(p^\infty)$ is also characterized as a group containing as subgroups all finite cyclic groups of order p^n $(n=1,2,\ldots)$, such that no proper subgroup of it possesses this property.

Since the subgroups of $\mathfrak{C}(p^\infty)$ are the $\mathfrak{C}(p^n)$, the factor groups of $\mathfrak{C}(p^\infty)$ are seen to be again $\mathfrak{C}(p^\infty)$ (and the zero group).

Take quasicyclic groups, one for each prime p, and form their direct sum:

$$\mathfrak{C} = \mathfrak{C}(2^\infty) + \mathfrak{C}(3^\infty) + \ldots + \mathfrak{C}(p^\infty) + \ldots .$$

This group is isomorphic to the multiplicative group of all complex roots of unity, or, otherwise expressed, to the group of all finite rotations of the circle.

SECTION 3

INTRODUCTORY THEOREMS

Theorem 0.1. Let T be the set of all elements of finite order in a group G. Then T is a torsion subgroup of G and the factor group G/T is torsion-free.

Proof: T is a torsion subgroup of G. For arbitrary elements a and b in T, there are integers m and n such that $ma = 0$ and $nb = 0$. From $mna = 0$, $mnb = 0$ we conclude $mn(a - b) = 0$; hence, $(a - b)$ has finite order r, a divisor of mn, and $(a - b)$ is an element of T. Thus $(a - b)$ is in T whenever $a,b \in T$.

The factor group G/T is torsion-free. Suppose $a + T$ is an element of G/T such that $n(a + T) \subseteq T$ for some positive integer n. Then the element na is in T and there is a positive integer m such that $m(na) = mn(a) = 0$. Hence a has finite order, $a \in T$, and $a + T = T$ is the zero element in G/T.

The subgroup T described in Theorem 0.1 is called the maximal torsion subgroup of G.

Theorem 0.2. If G is any torsion group, then G may be represented as a direct sum of p-groups. The direct summands are determined uniquely by G.

Proof: For each different prime p let G_p consist of all x in G whose order is a power of p. G_p is a subgroup of G. For any two elements x and y in G_p there are integers m and

n such that $p^m x = 0$ and $p^n y = 0$. If $m = n$, then $p^m(x - y) = 0$. If $m \neq n$, assume $m > n$, then $p^m(x - y) = 0$. In either case, $(x - y)$ is in G_p whenever $x,y \in G_p$. By our choice of elements for G_p, it is clear that G_p is a p-group.

Let G* be the direct sum of the various subgroups G_p, $G^* = \Sigma\, G_p$. We show that $G \cong G^*$. Let x be any element of G. Since G is a torsion group, x has finite order, say n. By the Fundamental Theorem of Arithmetic, n is expressible uniquely as the product of powers of prime numbers. Suppose

$$n = p_1^r p_2^s \cdots p_k^z$$

is the factored form for n, where the p_i are distinct prime numbers. Define $n_1 = n/(p_1^r)$; and make similar definitions for the remainder of the k prime numbers. In this manner we have constructed k numbers, $n_1, n_2, \ldots, n_k$, whose greatest common divisor is 1. Thus there are k integers $c_1, \ldots, c_k$, such that $c_1n_1 + c_2n_2 + \ldots + c_kn_k = 1$. Then we obtain $x = c_1n_1x + c_2n_2x + \ldots + c_kn_kx$. Recalling that $n_1 = n/(p_1^r)$, and that $O(x) = n$, we see that n_1x has order precisely p_1^r, and $n_1x \in G_{p_1}$. Similarly we find that

$$n_2x \in G_{p_2}\ ,\ n_3x \in G_{p_3}\ ,\ \ldots\ ,\ n_kx \in G_{p_k}\ .$$

Thus an arbitrary element $x \in G$ has been expressed as a sum of elements from the G_p. This representation is unique. To see this, assume the contrary; suppose

$$x = y_1 + y_2 + \ldots + y_k = z_1 + z_2 + \ldots + z_k$$

where y_i and z_i lie in the same G_{p_i} for each $i = 1, 2, \ldots, k$. Consider the equation

$$y_1 - z_1 = (z_2 + z_3 + \ldots + z_k) - (y_2 + y_3 + \ldots + y_k)$$

in which the order of the right member is a product of powers of $p_2, \ldots, p_k$ while the order of the left member is, a power of p_1. This is possible only if $y_1 = z_1$. By a similar argument we find that $y_i = z_i$ for each i.

The p-groups G_p that are uniquely determined by the group G are called the p-components of G.

Theorem 0.3. Let H be a subgroup of a group G. Suppose the factor group G/H is a direct sum, $G/H = \Sigma\, G_\lambda/H$, and that H is a direct summand of each G_λ, $G_\lambda = H + J_\lambda$. Then H is a direct summand of G and $G = H + \Sigma\, J_\lambda$.

Proof: It is clear that H and all the J_λ generate G. To see that G is their direct sum, suppose $h + x_1 + \ldots + x_n = 0$ with $h \in H$ and $x_i \in J_{\lambda_i}$. In G/H we obtain

$$x_1^* + x_2^* + \ldots + x_n^* = 0^*, \qquad (x^* = x + H).$$

Recalling that direct summands are disjoint (except for 0), we conclude

$$x_1^* = \ldots = x_n^* = 0^*$$

since the x_i^* belong to different direct summands G_λ/H of G. Thus x_i is in H and so x_i belongs to the intersection of H and the particular J_{λ_i} containing x_i. Since $H \cap J_{\lambda_i} = 0$, $x_i = 0$, and we finally obtain $h = 0$.

Theorem 0.4. The ranks $r(G)$, $r_0(G)$ and $r_p(G)$ are invariants of G and $r(G) = r_0(G) + \sum_{p=2,3,5,\ldots} r_p(G)$.

Proof: The validity of $r(G) = r_0(G) + \sum_{p=2,3,5,\ldots} r_p(G)$

follows from the fact that a maximal independent set L containing only elements of order infinity and/or of prime power order decomposes into its disjoint subsets L_o and L_p, one L_p for each prime p (where L_o consists of all elements in L whose order is infinite and L_p of those whose order is some power of p); furthermore, L_o and L_p (p = 2, 3, 5, ...) are independent sets maximal with respect to the property of containing elements of infinite or prime power order. Thus the statement of Theorem 0.4 must be verified only for the ranks $r_o(G)$ and $r_p(G)$.

$r_o(G)$ is invariant. We first reduce the proof to torsion-free groups by showing that $r_o(G) = r(G/T)$ where T is the maximal torsion subgroup of G. Let $a_1, \ldots, a_k \in G$ be independent of infinite order, and $a_i^* = a_i + T$. Then

$$m_1a_1^* + \ldots + m_ka_k^* = 0^* \text{ implies}$$

$$m_1a_1 + \ldots + m_ka_k = b \text{ for some } b \in T.$$

If $O(b) = n$, then

$$nm_1a_1 + \ldots + nm_ka_k = 0,$$

and by independence we obtain $nm_ia_i = 0$; then $m_i = 0$ for all i; hence $a_1^*, \ldots, a_k^*$ are independent in G/T. Conversely, if the a_i^* are independent and a_i is an arbitrary element of a_i^*, then

$$m_1a_1 + \ldots + m_ka_k = 0 \text{ implies}$$

$$m_1a_1^* + \ldots + m_ka_k^* = 0^*$$

and $m_i = 0$ for all i. Consequently $[a_\lambda^*]_{\lambda \in \Lambda}$ is a maximal independent set containing only elements of infinite order

in G and is maximal with respect to this property. Thus $r_o(G) = r(G/H)$ and we restrict ourselves to proving the uniqueness of r(G) for the case of torsion-free groups G.

Let G be torsion-free and $L = [a_\lambda]_{\lambda \in \Lambda}$, a maximal independent set in G; by definition, $r(G) = |\Lambda|$. If g is an arbitrary nonzero element of G, we have

$$ng = n_1 a_{\lambda_1} + \ldots + n_k a_{\lambda_k} \neq 0,$$

since g is dependent on L. If we associate with g the k-tuple $(\lambda_1, \ldots, \lambda_k)$ and the corresponding rational numbers $(r_1, \ldots, r_k)$ where $r_i = n_i n^{-1}$, then g is uniquely determined by them. In fact, if g' is some other element of G with the same $(\lambda_1, \ldots, \lambda_k)$ and $(r_1, \ldots, r_k)$, then

$$n'g' = n_1' a_{\lambda_1} + \ldots + n_k a_{\lambda_k} \text{ with } n_i' n'^{-1} = n_i n^{-1},$$

so that $nn'(g' - g) = 0$; i.e., $g' = g$, since the group is torsion-free. This inference shows that the power of G does not exceed the power of the set of all $(\lambda_1, \ldots, \lambda_k, r_1, \ldots, r_k)$, and thus we obtain the inequality $|G| \leq r(G) \cdot \aleph_o$. But also $r(G) \leq |G|$. Thus if r(G) is an infinite cardinal, then $r(G) = |G|$.

In addition, r(G) is invariant if r(G) is finite. To prove this we are in need of

Lemma 0.5 Let G be a torsion-free group, and $a_1, \ldots, a_k$ an independent set in G such that each a_i depends on $b_1, \ldots, b_s \in G$. Then $k \leq s$ and, after a suitable reordering of $b_1, \ldots, b_s$, the set $a_1, \ldots, a_k, b_{k+1}, \ldots, b_s$

is equivalent to $b_1, \ldots, b_s$.

Proof: The dependence of the a_i on $b_1, \ldots, b_s$ means that some nonzero multiple of a_i is a linear combination of $b_1, \ldots, b_s$, and the equvalence of two subsets denotes that all the elements of each subset depend on the other set.

Proof is by induction on k. For k = 0 the assertion is clear; assume it is true for k - 1. Since the hypotheses hold for $a_1, \ldots, a_{k-1}$ and $b_1, \ldots, b_s$ we may assume for example $a_1, \ldots, a_{k-1}, b_k, \ldots, b_s$ is equivalent to $b_1, \ldots, b_s$. By assumption, a_k depends on $b_1, \ldots, b_s$ and so on the equivalent set $a_1, \ldots, a_{k-1}, b_k, \ldots, b_s$ (G is torsion-free):

$$0 \neq na_k = m_1a_1 + \ldots + m_{k-1}a_{k-1} + m_kb_k + \ldots + m_sb_s.$$

The independence of the a_i implies $s \geq k$ and at least one of the $m_k, \ldots, m_s$ differ from 0, say $m_k \neq 0$. Then

$$m_kb_k = -m_1a_1 - \ldots -m_{k-1}a_{k-1} + na_k -m_{k+1}a_{k+1} - \ldots -m_sb_s$$

shows that b_k depends on $a_1, \ldots, a_k, b_{k+1}, \ldots, b_s$ which is thus equivalent to $a_1, \ldots, a_{k-1}, b_k, \ldots, b_s$. The latter set is equivalent to $b_1, \ldots, b_s$; consequently, so is the former, and the proof of Lemma 0.5 is complete.

Lemma 0.5 demonstrates that if $a_1, \ldots, a_k$ and $b_i, \ldots, b_s$ are independent, equivalent sets in the torsion-free group G, then k = s. Since two maximal independent sets are equivalent, r(G) does not depend on the choice of the maximal independent set (if r(G) is finite). Thus

$r_o(G)$ is invariant for all groups G.

$r_p(G)$ is an invariant. Evidently $r_p(G) = r(T_p)$ where T_p denotes the p-component of the maximal torsion subgroup T of G. Thus we consider only p-groups G and prove the invariance of r(G) for this case.

A group is said to be <u>simple</u> if the only normal or invariant subgroups of G are itself and the identity subgroup. Since an abelian group is simple if and only if it is a cyclic group of prime order, the socle S(G) of a p-group is G[p]. This property of S(G) will be regarded as the definition of S(G).

Let S(G) be the socle of the p-group G, then $r(G) = r(S(G))$. A set $a_1, \ldots, a_k \in G$ is independent if and only if

$$p^{n_1-1}a_1, p^{n_2-1}a_2, \ldots, p^{n_k-1}a_k \qquad (n_i = E(a_i))$$

are independent. Thus only the uniqueness of r(S(G)) needs a verification.

If $L = [a_\lambda]_{\lambda\in\Lambda}$ is a maximal independent set in S(G), then every nonzero element $g \in S(G)$ may be written in the form $g = n_1a_{\lambda_1} + \ldots + n_ka_{\lambda_k}$ with $0 \leq n_i \leq p-1$. Indeed, g depends on L, so that $ng = m_1a_{\lambda_1} + \ldots + m_ka_{\lambda_k} \neq 0$.

Since $(n,p) = 1$, there is an integer t with $nt \equiv 1 \pmod p$, so that $g = ntg = (m_1t)a_{\lambda_1} + \ldots + (m_kt)a_{\lambda_k}$. The unicity is a consequence of independence. We conclude that if $r(S(G)) = r$ is finite, then $|S(G)| = p^r$ and if r(S(G)) is infinite, then $r(S(G)) = |S(G)|$. This proves that r(S(G)) and so r(G)

is an invariant of G.

Theorem 0.6 A subset $[a_\lambda]_{\lambda\in\Lambda}$ of G is independent if and only if the subgroup generated by the a_λ is the direct sum of the $\{a_\lambda\}$.

Proof: If $\{\ldots, a_\lambda, \ldots\} = \Sigma\{a_\lambda\}$, then $m_1a_{\lambda_1} + \ldots + m_ka_{\lambda_k} = 0$ implies $m_1a_{\lambda_1} = \ldots = m_ka_{\lambda_k} = 0$, because each $m_ia_{\lambda_i}$ belongs to a different direct summand. Conversely, if the $a_\lambda(\lambda\in\Lambda)$ are independent, then, for each $\lambda\in\Lambda$, the intersection of $\{a_\lambda\}$ with $\{\ldots, a_\mu, \ldots\}$ is the direct sum of the $\{a_\lambda\}$.

If $G = \Sigma\{a_\lambda\}$, then $[a_\lambda]_{\lambda\in\Lambda}$ is a basis of G.

In theorem 0.4, our inference shows that in S(G) any maximal independent set generates S(G). Hence Theorem 0.6 implies Theorem 0.7.

Theorem 0.7 If G is a group satisfying pG = 0 for some prime p, then any maximal independent set $[a_\lambda]$ in G is a basis of G; i.e., $G = \Sigma\{a_\lambda\}$.

Theorem 0.8 A subset B of a group G is a basis of G if and only if

i) it is a maximal independent system of G,

ii) no element of B can be replaced by an element of a greater order, relative to B, without violating independence.

Proof: Suppose $B = [a_\lambda]_{\lambda\in\Lambda}$ is a basis of G; i.e., B is an independent set which generates G. Then i) is satisfied by definition. If b is any nonzero element of G, we have

(1) $b = m_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k}$ (with $m_i a_\lambda \neq 0$, $k \geq 1$)

for some $a_{\lambda_1}, \ldots, a_{\lambda_k} \in B$, since B generates G. None of the $a_\lambda \in B$ other than one of the $a_{\lambda_1}, \ldots, a_{\lambda_k}$ can be replaced by b without violating independence. For this would imply that b, an element of an independent set, could be written in the form (1); i.e., as a linear combination of other elements of the independent set. If $O(a_{\lambda_i}) < O(b)$, then multiplying (1) by $O(a_{\lambda_i}) = n \neq 0$, we see that this a_{λ_i} cannot be replaced by b since

$$nb = nm_1 a_{\lambda_1} + \ldots + nm_k a_{\lambda_k} \text{ would mean}$$

$$0 = -nb + nm_1 a_{\lambda_1} + \ldots + nm_{i-1} a_{\lambda_{i-1}} + nm_{i+1} a_{\lambda_{i+1}} + \ldots + nm_k a_{\lambda_k},$$

clearly a violation of independence. Finally, if

$$O(a) = O(b) = \infty,$$

then $|m_i| \geq |1|$ implies that b is not of a greater order than a_{λ_i}, relative to B.

Conversely, let $B = [a_\lambda]_{\lambda \in \Lambda}$ be a subset of G with the properties i), ii). The maximal independent set generates the direct sum $H = \Sigma \{a_\lambda\}$ in G.

H = G. Suppose $H \neq G$, then there is an element $b \in G$ such that $b \notin H$. By i), some multiple of b is in H. We may assume

(2) $$pb = m_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k}$$

where $a_{\lambda_i} \in B$, $m_i a_{\lambda_i} \neq 0$, $k \geq 0$, and p is a prime. For if

$$nb = m_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k}$$

with n a composite, then $n = p_1^{c_1} p_2^{c_2} \ldots p_r^{c_r}$. Then

$$nb = (p_1^{c_1} p_2^{c_2} \ldots p_r^{c_r})b = p_i(p_1^{c_1} \ldots p_i^{c_{i-1}} \ldots p_r^{c_r})b$$

We may alter the choice of b to the element $(p_1^{c_r} \ldots p_i^{c_{i-1}} \ldots p_r^{c_r})b$ and let $p_i = p$ to obtain (2). In addition, we may assume $0 < |m_i| < p$, for suppose $m_i a_{\lambda_i}$ in (2) may be written as px with $x \varepsilon H$. Then replace b with B' + x to obtain

$$p(b' + x) = m_1 a_{\lambda_1} + \ldots + px + \ldots + m_k a_{\lambda_k} \text{ or}$$

$$pb' = m_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k}$$

where $px = m_i a_{\lambda_i}$ has been deleted in the sum on the right. This b' satisfies $b' \notin H$, $pb' \varepsilon H$.

Now if in (2) $O(a_{\lambda_i}) = \infty$, then $O(b) = \infty$ and since $|m_i| < p$, b is of greater order than a_{λ_i} relative to B. The replacement of a_{λ_i} by b will not affect the independence of the system. Because of ii) there is no a_{λ_i} of infinite order in (2).

If the a_{λ_i} in (2) are of finite order, then we may assume that all $O(a_{\lambda_i})$ are powers of the prime p. Let $O(a_{\lambda_i}) = p^r \geq O(a_{\lambda_i})$ for i = 2,3,...k. From (2) we obtain $p^r b = m_1 p^{r-1} a_{\lambda_1} + \ldots + m_k p^{r-1} a_{\lambda_k}$ which is not zero, since (mp) = 1. It follows that $O(b) > O(a_{\lambda_1})$, and a_{λ_1} can be replaced by b without disturbing the independence of B. In view of ii), there is no a_{λ_i} in (2), and (2) reduces to pb = 0. By i), b depends on, and so is expressible in terms of, $[a_\lambda]_{\lambda \varepsilon \Lambda}$, i.e., $b \varepsilon H$, and H = G.

Theorem 0.9 A subset B of a group G is a basis of G if and only if

iii) it is a generating system not containing O,

iv) no element a_λ of B can be replaced by an element of smaller order, relative to a'_λ, so as to get again a generating system of G. (Here a_λ is considered as an independent set consisting of a single element. If a_λ is of infinite order, then b is of a greater order than a_λ if $rb = sa \neq 0$ holds with $|r| > |s|$).

Proof: B is a minimal generating system since any unnecessary nonzero element of B could be replaced by O.

Let $B = [a_\lambda]_{\lambda \varepsilon \Lambda}$ be a basis of G. Then iii) is clear. Let b be a nonzero element of G and write b in the form

(1) $\quad b = m_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k} \quad (m_i a_{\lambda_i} \neq 0,\ k \geq 1)$

for some $a_{\lambda_1}, \ldots, a_{\lambda_k} \varepsilon B$. First, let O(b) be finite; then a_{λ_i} $(i = 1,\ldots,k)$ can be replaced by b (so as to again obtain a generating system) only if $(m_i, O(a_{\lambda_i})) = 1$. Evidently, $O(b) \geq O(m_i a_{\lambda_i})$ and $O(m_i a_{\lambda_i})$ is equal to $O(a_{\lambda_i})$ if m_i is relatively prime to $O(a_{\lambda_i})$. Thus only b of a greater or equal order can replace a_{λ_i}. Secondly, if $O(b) = \infty$, and b is of a smaller order than $a_\lambda \varepsilon B$, relative to a_λ, then $mb = na_\lambda$ with $|m| < |n|$, and so in (1) only one a_λ of infinite order occurs and its coefficient is greater than 1 in absolute value. But then a_λ does not

belong to the group generated by B with a_λ replaced by b. Thus iv) follows.

Conversely, let $B = [a_\lambda]_{\lambda \varepsilon \Lambda}$ satisfy iii), iv). Then we show

(5) $\quad n_1 a_{\lambda_1} + \ldots + m_k a_{\lambda_k} = 0 \quad (n_i a_{\lambda_i} \neq 0,\ k \geqq 1)$

is impossible. If $O(a_{\lambda_i}) = \infty$, then we may replace $a_{\lambda_i} \varepsilon B$ by $(1 + |n_i|)a_{\lambda_i}$ which is of a smaller order than a_{λ_i}, relative to a_{λ_i}, and we obtain again a generating system of G, since $|n_i| a_{\lambda_i}$ is expressible by other a_λ and so a_{λ_i} belongs to the group generated by the new system. Consequently, we may assume that in (2) the orders of the a_{λ_i} are powers of some prime p. Let p^t $(t \geqq 0)$ be the greatest power dividing every n; put $n_i = p^t n_i'$ and assume $(n_1', p) = 1$, for example.

Then

$$b = n_1' a_{\lambda_1} + \ldots + n_k' a_{\lambda_k}$$

satisfies $O(b) \leqq p^t < O(a_{\lambda_1})$ and, since $(n_1', p) = 1$, if we replace a_{λ_1} by b in B, we shall again get a generating system for G. We have thus derived a contradiction to iv) and the theorem follows.

CHAPTER 1

DIRECT SUMS OF CYCLIC GROUPS

SECTION 1

FREE GROUPS

Let $S = [a_\lambda]_{\lambda \in \Lambda}$ be a non-empty set of elements. The free group F generated by S is the group with the following properties:

i) F is generated by S, and

ii) If G is any group generated by a set of elements X and if there is a one-to-one correspondence between S and X, $S \Leftrightarrow X$, then there is a homomorphism η of F onto G, $\eta : F \to G$, taking S onto X.

A free group is the direct sum of any number of infinite cyclic groups $\{a_\lambda\}$ $(\lambda \in \Lambda)$; F consists of all finite linear combinations $n_1 a_{\lambda_1} + n_2 a_{\lambda_2} + n_3 a_{\lambda_3} + \dots + n_k a_{\lambda_k}$ with different a_λ, where the n_i are arbitrary nonzero integers and k is a non-negative integer. Equality is defined by formal coincidence, and the addition of the linear combinations is performed formally by adding the coefficients of the same a_λ. The set S is called a free set of generators of F. We observe that although F does depend on the power of the index set Λ, it is independent of our choice of the particular elements a_λ. The generators a_λ constitute a maximal independent set

in F and we have $r(F) = |\Lambda|$, and any two free groups with the same rank are isomorphic. The symbol F(m) denotes a free group of rank m. Thus, for free groups, the rank serves as a characteristic invariant since the rank m of F completely determines (up to isomorphism) the group F.

Suppose η : F(m) $\rightarrow$ G is a homomorphism of F(m) onto G. Then G is isomorphic to F(m)/K where K is the kernel of the homomorphism η ; i.e., K: $\{x \in F(m) | x\eta = 0\}$. Let the genrators of G be $g_1, \ldots, g_m$. Suppose F(m) has generators $a_{\lambda_1}, \ldots, a_{\lambda_m}$ and that $a_{\lambda_i} = g_i$ for $i = 1,2,\ldots, m$. An element of K has the form $u_1 a_{\lambda_1} + \ldots + u_m a_{\lambda_m}$; its image under η is at once 0 and $u_1 g_1 + \ldots + u_m g_m$. The expression $u_1 g_1 + \ldots + u_m g_m$ such that $u_1 a_{\lambda_1} + \ldots + u_m a_{\lambda_m} \in K$ is called a <u>defining relation</u> of G relative to the generating system $[g_\lambda]_{\lambda \in \Lambda}$.

<u>Theorem 1.1</u> If the factor G/H is free, then G is the direct sum of H and a free group F, G = H + F.

<u>Proof</u>: By Theorem 0.3, all we need show is that H is a direct summand of G if G/H is an infinite cyclic group, $G/H = \{a^*\}$. Taking $a \in a^*$, we see that the cosets ka^*/H where k ranges over the integers are represented by the elements ka of $\{a\}$ so that $G = H + \{a\}$, since distinct cosets are disjoint and each element of G is in H or a coset of H in G.

<u>Theorem 1.2</u> Let F be a free group mapped by a homomorphism η into a group H, and let G be any group mapped by a homo-

morphism Θ onto H, then there exists a homomorphism x of F into G such that $\eta = \Theta x$; i.e., $\eta = \Theta x$ has a solution.

Proof: For each generator a_λ of F, the homomorphism η associates with it an element $a_\lambda \eta = h \in H$. Since the homomorphism Θ is onto, it is always possible to choose some g_λ in G with $g_\lambda \Theta = a_\lambda$. Let x be induced by the correspondence $a_\lambda \longrightarrow g_\lambda$. By the freeness of F this is, in fact, a homomorphism and it has the required property.

SECTION 2

FINITE GROUPS

In this section we examine the structure of finite groups. The main result covers the entire class of finite groups. A finite group is of necessity a torsion group, and so by Theorem 0.2, we may confine our attention to finite p-groups.

Lemma 1.3 If G is a finite p-group and a is an element of maximal order p^k, then $\{a\}$ is a direct summand of G.

Proof: Suppose a is an element of maximal order p^k in G. Let H be a maximal subgroup with respect to the property $H \cap \{a\} = 0$. Then $G^* = \{H, a\} = H + \{a\}$. We show that $G = G^*$. If G^* is a proper subgroup of G, then there is an element x in G such that $x \notin G^*$. We may assume, without loss of generality, that $px \in G^*$, for if not, we could replace x with one of its multiples which does satisfy the desired requirement. We are assured of the existence of

such a multiple since G was assumed to be finite, and the maximal order possible for any element is p^k. Since $px \in G^*$, we have $px = h + na$ where $h \in H$, n is an integer. In view of the maximality of p^k,

$$p^{k-1}h + p^{k-1}na = p^{k-1}(px) = 0 \quad (p^{k-1}h \in H,\ p^{k-1}na \in \{a\}).$$

Recalling that $H \cap \{a\} = 0$, we conclude $p^{k-1}h = p^{k-1}na = 0$. p^k divides $p^{k-1}n$ since by hypothesis $O(a) = p^k$, $p^k a = 0$, i.e., $n = pj$ for some integer j. From $px = h + na$, we have $px - na = h$, $px - pja = h$, $p(x - ja) = h \in H$. But $x - ja \notin H$ since $x \notin G^*$, $ja \in \{a\}$, and $H \cap \{a\} = 0$. By the maximality of H, $\{H,(x - ja)\}$ contains a nonzero element ra of $\{a\}$. Thus

(1) $ra = h' + s(x - ja)$, $(h' \text{ in } H)$, or

(2) $sx = -h' + (r - sj)a$ $(-h' \in H,\ (r - sj)a \in \{a\})$.

From (2) we conclude $sx \in H + \{a\}$ where we must have $(s,p) = 1$ in order that the hypothesis $H \cap \{a\} = 0$ is not contradicted. Because $(s,p) = 1$, there are integers m and n such that $ms + np = 1$, $msx + npx = x$. Now $sx \in G^*$ and $px \in G^*$ imply that $x \in G^*$, a contradiction. We conclude $G = G^*$.

Theorem 1.4 A finite group G is the direct sum of a finite number of cyclic groups of prime power order.

Proof: We choose in G an element of maximal order p^k and write $G = H + \{a\}$ according to Lemma 1.3. We repeat the process for H, which is of smaller order. This yields the desired result in a finite number of steps because G is finite.

SECTION 3

FINITELY GENERATED GROUPS

The structure of any finitely generated group is described in Theorem 1.6. We need

Lemma 1.5 If $A = \{a_1, \ldots, a_k\}$, and $n_1, \ldots, n_k$ are arbitrary integers with greatest common divisor 1, then A may be written in the form $A = \{b_1, \ldots, b_k\}$ where $b_1 = n_1a_1 + \ldots \ldots + n_ka_k$.

Proof: The statement is clear if $n = |n_1| + \ldots + |n_k| = 1$; i.e., if all but one of the n_i vanish and the nonzero n_i is ± 1. We assume $n > 1$ and we use induction on n. Now $n > 1$ and $(n_1, \ldots, n_k) = 1$ imply that at least two of the n_i do not vanish, say $|n_1| \geq |n_2| > 0$. Then we have either $|n_1 + n_2| < n_1$ or $|n_1 - n_2| < n_1$, and it follows that

$$|n_1 \pm n_2| + |n_2| + \ldots + |n_k| < n$$

for one of the two signs. The induction hypothesis and $(n_1 \pm n_2, n_2, \ldots, n_k) = 1$ imply

$$A = \{a_1, \ldots, a_k\} = \{a_1, a_2 \pm a_1, a_3, \ldots, a_k\}$$

$$= \{b_1, b_2, \ldots, b_k\} \text{ with}$$

$$b_1 = (n_1 \pm n_2)a_1 + n_2(a_2 \mp a_1) + n_3a_3 + \ldots + n_ka_k$$

$$= n_1a_1 + n_2a_2 + \ldots + n_ka_k,$$

completing the proof of the lemma.

Theorem 1.6 A finitely generated group G is the direct sum of a finite number of cyclic groups of infinite and/or prime

power order.

Proof: Consider in the finitely generated group G all generating systems $g_1, \ldots, g_k$ with a fixed number k of elements, and choose a generating system $a_1, \ldots, a_k$ such that the system of orders $O(a_1), O(a_2), \ldots, O(a_k)$ is lexicographically the first of all such systems; i.e., $O(a_1) \leq \ldots \leq O(a_k)$ and no generating system $g_1, \ldots, g_k$ exists in G with $O(g_1) \leq \ldots \leq O(g_k)$ which satisfies $O(a_1) = O(g_1), \ldots, O(a_{i-1}) = O(g_{i-1}), O(a_i) < O(g_i)$ for some i. We prove that G is the direct sum of the cyclic subgroups generated by the generators a_i. First we observe that the a_i constitute a generating system so that any element of G may certainly be written as a linear combination of the a_i. Secondly, we observe that the a_i are independent. For suppose not; then $m_j a_j + \ldots + m_k a_k = 0$ with $m_j a_j \neq 0$. We may assume $0 < m_j < O(a_j)$, set $(m_j, \ldots, m_k) = m$, and let $m_i = mn_i$. Then $(n_j, \ldots, n_k) = 1$ and we may apply Lemma 1.5 to conclude that $\{a_j, \ldots, a_k\} = \{b_j, \ldots, b_k\}$ where $b_j = n_j a_j + \ldots + n_k a_k$. Now

$$mb_j = mn_j a_j + \ldots + mn_k a_k = m_j a_j + \ldots + m_k a_k = 0$$

and it follows that

$$G = \{a_1, \ldots, a_{j-1}, a_j, \ldots, a_k\}$$
$$= \{a_1, \ldots, a_{j-1}, b_j, \ldots, b_k\}$$

with $O(b_j) \leq m \leq m_j < O(a_j)$ which contradicts the definition of the elements a_i.

As a point of interest, we remark that it can be

shown that the representation of a finitely generated group as a direct sum of groups $\mathcal{C}(\infty)$ and $\mathcal{C}(p^k)$ is uniquely determined (up to isomorphism, of course). The orders of these uniquely determined groups of infinite and/or prime power order are called the invariants of G. Two finitely generated groups are isomorphic if and only if their invariants match.

SECTION 4

DIRECT SUMS OF CYCLIC p-GROUPS

In the next chapter we will consider divisibility in a group. For our present purpose, a simple definition will serve. An element x of a group G is said to be divisible by the integer n if there exists an element $y \in G$ such that $ny = x$. Observe that the concepts of divisibility and height are closely related. Recall that by the p-socle of a p-group we mean the set of all elements $g \in G$ for which $pg = 0$. The p-socle of a group G is denoted G[p].

Theorem 1.7 A p-group G is a direct sum of cyclic groups if and only if G is the union of an ascending chain of subgroups G_n $(n = 1,2, \ldots)$ such that the height of every nonzero element in G_n is at most a finite number k_n (which may depend on n).

Proof: Let G be a direct sum of cyclic p-groups. Collect in one such decomposition the cyclic direct summands of the same order p^n, for each n, and denote their direct sum

by A_n. If we put $G_n = A_1 + \ldots + A_n$, then the G_n satisfy the conditions in the theorem with $k_n = n - 1$.

Conversely, assume the p-group G to be the union of an ascending chain of subgroups G_n $(n = 1, 2, \ldots)$ such that the heights of the nonzero elements in G are at most k_n. Form the p-socle P_n of G_n and pick from $P_1 \cap (p^{k_1}G)$ a maximal independent set of elements; then expand this independent set in turn with elements of $P_1 \cap p^{k_1-1}G, \ldots, P_1 \cap pG, P_1$ to an independent set S_1 which is in each step maximal. Next proceed to P_2 and extend S_1 in $P_2 \cap p^{k_2}G$, then in $P_2 \cap p^{k_2-1}G, \ldots, P_2 \cap pG, P_2$ so that the independent set obtained after each step is maximal. Then repeat this process with the set S_2 thus constructed, and so on. Finally let S be the union of all these S_n $(n = 1,2, \ldots)$. Denote the elements of S by c_λ $(\lambda \in \Lambda)$. With each c_λ associate the element $a_\lambda \in G$ which satisfies $p^{m_\lambda}a_\lambda = c_\lambda$ where $m_\lambda = H(c_\lambda)$. Then the set $[a_\lambda]_{\lambda \in \Lambda}$ is again independent. If not, we could find a nontrivial linear relation among the a_λ. Since the heights m_λ are finite, we could multiply this relation among the a_λ by the maximum height involved and obtain a nontrivial relation among the c_λ, a contradiction. Considering that $P = G[p]$ is the union of the P_n, from Theorem 0.7 we obtain $P = \sum_\lambda \{c_\lambda\}$. We show that $G' = \sum_\lambda \{a_\lambda\} = G$. Assume there exists an element g which belongs to G but not to G'. Suppose g has order p^k. Then $p^{k-1}g \in P$ since $p(p^{k-1}g) = p^k g = 0$, and we can write

(1) $p^{k-1}g = r_1c_1 + \ldots + r_tc_t \quad (c_i \in S,\ 0 < r_i < p)$.

If here some c_i satisfies $H(c_i) \geq k - 1$, we may exchange g for $g - (r_i'a_i)$ $(r_ic_i = p^{k-1}r_i'a_i)$ which also does not belong to G' and satisfies an equation like (1). Thus we suppose that in (1) all c_i satisfy $H(c_i) \leq k - 2$. Surely $t \geq 1$, for otherwise $p^{k-1}g = 0$, so that the order of g is p^{k-1}. We conclude that $g \in G'$ because $O(g) < p^k$ and g was chosen with smallest order p^k. The c_i belong to some S_μ. If μ is as small as possible, then there is a c_i, say c_t, not in $S_{\mu-1}$. Now $p^{k-1}g$ lies in P_μ and is of greater height than c_t, so that in the construction of S_μ, $p^{k-1}g$ was taken into consideration earlier then c_t. By construction, $p^{k-1}g$ must depend on and hence is expressible by elements c_λ chosen before c_t. But then $p^{k-1}g$ is also a linear combination of the c_λ where c_t does not appear, in contradiction to the independence of the set $[c_\lambda]_{\lambda \in \Lambda}$.

A <u>bounded group</u> (or a group of bounded order) is, in the first place, a torsion group, so that all of its elements have finite order, with the restriction that there is a fixed upper bound to the orders of the elements. In other words, there is a positive integer n such that $nx = 0$ for all x, or, more briefly, such that $nG = 0$. Any finite group is of bounded order. An infinite group can also be of bounded order. To see this, take the direct sum of an infinite number of finite cyclic groups, having an upper bound on the orders of the summands.

Theorem 1.8 A bounded group is a direct sum of cyclic groups.

Proof: Let A be a bounded p-group. Form an ascending chain with each member being the group A itself. We obtain $A \subseteq A \subseteq \ldots$. A has been expressed as the union of an ascending chain of subgroups. By hypothesis, the height of the nonzero elements in A remain under a finite bound. Our conclusion follows by Theorem 1.7.

Theorem 1.9 (Prüfer) A countable p-group is a direct sum of cyclic groups if and only if it contains no nonzero elements of infinite height.

Proof: Suppose G is a countable p-group which is the direct sum of cyclic groups. G has no nonzero elements of infinite height. Select a generating system $g_1, g_2, \ldots, g_n, \ldots$ of G. Set $G_1 = \{g_1\}$, $G_2 = \{g_1, g_2\}$, $\ldots$, $G_n = \{g_1, \ldots, g_n\}$, $\ldots$, then $G = G_1 \cup G_2 \cup \ldots \cup G_n \cup \ldots$. Since G is a p-group, the heights of the elements in G_n are bounded. If $x \in G$, x is in some G_n and x has finite height. Conversely, if G is a countable p-group without nonzero elements of infinite height, then G is a direct sum of cyclic groups by a direct application of Theorem 1.7.

Theorem 1.10 Any two decompositions of a group G into direct sums of cyclic groups (of infinite and/or prime power order) are isomorphic.

Proof: We consider first the set of direct summands of prime power order. Denote by P_n the subgroup of $P = G[p]$

which consists of elements of height $\geq n - 1$. If G is a direct sum of cyclic p-groups, then P_n is the direct sum of the socles of all these direct components whose order is not less than p^n; and so P_n/P_{n+1} is isomorphic to the direct sum of the socles of all components of order just p^n. We see that the number of cyclic direct summands of order p^n in a direct decomposition of G is equal to the rank of P_n/P_{n+1}. Since the P_n are defined without reference to the direct decomposition, we are led to the conclusion desired.

We have still to prove that the power of the set of infinite cyclic direct summands is always the same. But this power is nothing else than the torsion-free rank of G.

SECTION 5

SUBGROUPS OF DIRECT SUMS OF CYCLIC GROUPS

From the results of the last two sections, we infer that if G is finitely generated, then not only G itself, but also every subgroup of G is again the direct sum of cyclic groups. By Theorem 1.9, the same is true for subgroups of countable torsion groups. We show that this is generally true. First we take up the torsion-free case.

Theorem 1.11 Every subgroup of a free group is free.

Proof: Let $G = \sum_{\lambda \in \Lambda} \{a_\lambda\}$ and suppose the index set Λ is well-ordered in some way. For ordinals α ($|\alpha| \leq |G|$), we define $G_\alpha = \sum_{\lambda \in \Lambda} \{a_\lambda\}$ and put $H_\alpha = H \cap G_\alpha$ for a suitable

subgroup H. Then $H_\alpha \subseteq H_{\alpha+1}$, $H_\alpha = H_{\alpha+1} \cap G_\alpha$, and, therefore, $H_{\alpha+1}/H_\alpha \cong \{H_{\alpha+1}, G_\alpha\} / G_\alpha$. This factor group is isomorphic to some subgroup of $G_{\alpha+1}/G_\alpha \cong \{a_\alpha\}$. Thus, either $H_{\alpha+1} = H_\alpha$ or $H_{\alpha+1}/H_\alpha$ is an infinite cyclic group. In the latter case by Theorem 1.1, we have $H_{\alpha+1} = H_\alpha + \{b_\alpha\}$, and if we let $b_\alpha = 0$ in case $H_{\alpha+1} = H_\alpha$, then it follows that the b_α generate the direct sum $\Sigma \{b_\alpha\}$. Since H is the union of the H_α, this direct sum equals H.

Theorem 1.12 Suppose the group G is the direct sum of cyclic groups. Any subgroup H of G is also the direct sum of cyclic groups.

Proof: First let us consider the case in which G is a p-group. Let G be the union of its subgroups, $G_1 \subseteq G_2 \subseteq \ldots$, where the heights of the elements in G_n are k_n. Then H is the union of the ascending chain $H_1 \subseteq H_2 \subseteq \ldots$ with $H_n = H \cap G_n$ and the heights of the elements in H_n taken in H do not exceed k_n. Application of Theorem 1.7 assures us that H is a direct sum of cyclic groups. The results can easily be extended to arbitrary torsion groups.

Suppose now that G is an arbitrary direct sum of cyclic groups and that T is its maximal torsion subgroup. Then $H \cap T$ is the maximal torsion subgroup of the subgroup H of G and $H/(H \cap T) \cong \{H,T\}/T$ is isomorphic to some subgroup of the free group G/T. Hence $H/(H \cap T)$ is free by Theorem 1.11 and by Theorem 1.1, H is the direct

sum of $H \cap T$ and a free group. In the preceding paragraph, we saw that $H \cap T$ is a direct sum of cyclic groups.

Corollary 1.13 Let G be the direct sum of cyclic groups. Then any two decompositions of G have isomorphic refinements.

Proof: Each direct summand is by Theorem 1.12 a direct sum of cyclic groups. If for each direct summand we substitute its direct decomposition into cyclic groups, we obtain refinements which are by Theorem 1.10 isomorphic.

Theorem 1.14 Suppose that the subgroup H of a group G is a direct sum of cyclic groups. Suppose, further, that for some positive integer n we have $nG \subseteq H \subseteq G$. Then G itself is a direct sum of cyclic groups.

Proof: Let H be a sub-group and n a positive integer which satisfies the hypothesis. By Theorem 1.12, nG is the direct sum of cyclic groups. Thus, it is sufficient to prove the theorem in the case $H = nG$. It is enough to do this in the case that n is a prime p.

Let $pG = \sum_{\lambda \varepsilon \Lambda} \{g_\lambda\}$ and choose elements a_λ in G with $pa_\lambda = g_\lambda$. Next extend the independent set $[a_\lambda]_{\lambda \varepsilon \Lambda}$ by elements $b_\mu (\mu \varepsilon M)$ of G[p] to obtain an independent set which is maximal in G. We now show that G is the direct sum of the cyclic groups $\Sigma \{a_\lambda\}$ $(\lambda \varepsilon \Lambda)$ and $\Sigma \{b_\mu\}$ $(\mu \varepsilon M)$. Since the sets $[a_\lambda]_{\lambda \varepsilon \Lambda}$ and $[b_\mu]_{\mu \varepsilon M}$ are independent, we have only to show that every $x \varepsilon G$ lies in their direct sum. Now px belongs to $pG = \Sigma \{g_\lambda\}$;

so we may write

$$px = n_1 g_{\lambda_1} + \ldots + n_r g_{\lambda_r} = n_1(pa_{\lambda_1}) + \ldots + n_r(pa_{\lambda_r})$$

We now have $py = 0$; i.e., $y \in G[p]$ and, thus, y is dependent on $[b_\mu]$. The maximality of the chosen independent set implies that y depends on, and therefore is expressible in terms of, the a_λ and $b_{\mu x}$, and so the same is true for x.

Corollary 1.15 Any group G is the union of an ascending sequence of subgroups, $G_1 \subseteq G_2 \subseteq \ldots \subseteq G_n \subseteq \ldots$, where every G_n is a direct sum of cyclic groups.

Proof: Define G_1 as a subgroup generated by an arbitrary maximal independent subset of G. If G_{n-1} is defined, let G_n consist of all $x \in G$ with $nx \in G_{n-1}$ $(n = 2, 3, \ldots)$. Then $nG_n \subseteq G_{n-1}$, and if G_{n-1} is a direct sum of cyclic groups, then so is G_n by the preceding result. That G is the union of the subgroups, G_n $(n = 1, 2, \ldots)$ follows at once from the choice of G_1.

SECTION 6

EXISTENCE OF A BASIS

In Section 1 of Chapter 0, we defined a basis; we now consider certain criteria for the existence of a basis.

The first criterion applies to p-groups. Suppose $L = [a_\lambda]_{\lambda \in \Lambda}$ is a maximal independent set of elements with the property that no element of L can be replaced by another group element with a greater height without

violating independence then L is called a <u>principal system</u>.

<u>Theorem 1.16</u> A p-group G containing no nonzero elements of infinite height is a direct sum of cyclic groups if and only if G contains a principal system.

<u>Proof</u>: We observe that a principal system is a subset of the socle; for if not, then an element can be replaced by its p-fold which is of greater height and is not O. By considering the definition, we see that if $B = [a_\lambda]_{\lambda \varepsilon \Lambda}$ is a basis of the p-group G, then $P = [p^{n_\lambda - 1} a_\lambda]_{\lambda \varepsilon \Lambda}$ is a principal system where $n_\lambda = E(a_\lambda)$. Conversely, let $P = [c_\lambda]_{\lambda \varepsilon \Lambda}$ be a principal system in G and suppose $a_{\lambda_1}{}_{\lambda \varepsilon \Lambda}$ are elements satisfying $p^{m_\lambda} a_\lambda = c_\lambda$ where $m_\lambda = H(c_\lambda)$; then $B = [a_\lambda]_{\lambda \varepsilon M}$ is a basis for G. Suppose B is not a basis. Then there is an element $g \varepsilon G$ which is not in the group generated by the elements in the set B. Choose g in such a way that g is an element of a smallest order p^r with this property. Then we have

$$p^{r-1} g = m_1 c_{\lambda_1} + \ldots + m_s c_{\lambda_s} \qquad (m_i \neq O)$$

for some $c_{\lambda_1}, \ldots, c_{\lambda_s} \varepsilon P$. If, in P, we replace one of the $c_{\lambda_1}, \ldots, c_{\lambda_s}$ by $p^{r-1} g$, the resulting set is independent and, therefore, by definition, we must have $H(c_{\lambda_i}) \geq r-1$. Putting

$$m_i c_{\lambda_i} = p^{r-1} m_i' a_{\lambda_i}$$

we see that

$$g' = g - m_1' a_{\lambda_1} - \ldots - m_s' a_{\lambda_s}$$

is of a smaller order than g, and, therefore $g' \varepsilon \{B\}$. But then also $g \varepsilon \{B\}$ and B is a basis for G.

For countable torsion-free groups we have

Theorem 1.17 A countable torsion-free group G is free if and only if each of its subgroups of finite rank is free.

Proof: The necessity follows from Theorem 1.11. For the sufficiency, consider a countable torsion-free group G with the property that each of its subgroups of finite rank is free. If G is of finite rank, then since G is a subgroup of itself by hypothesis, it is free. Let $c_1, \ldots, c_n, \ldots$ be a maximal independent set in G and consider the set of all $b \varepsilon G$ satisfying a relation $kb = k_1c_1 + \ldots + k_rc_r$ $(k_r \neq 0)$ with a fixed r. Since these b are included in a subgroup of rank no greater than r, our hypothesis guarantees the existence of a fixed integer $m \neq 0$ with $mb \varepsilon \{c_1, \ldots, c_r\}$ for every b considered. Write $mb = m_1c_1 + \ldots + m_rc_r$ $(m_r \neq 0)$ and select a $b = b_r$ with a minimal value of $|m_r|$. It follows that the set $b_1, \ldots, b_n, \ldots$ is independent, for we have $b_1 = m_{11}c_1$ $(m_{11} \neq 0)$, $b_2 = m_{21}c_1 + m_{22}c_2 (m_{22} \neq 0)$, $\ldots$, $b_n = m_{n1}c_1 + m_{n2}c_2 + \ldots + m_{nn}c_n$ $(m_{nn} \neq 0)$, ... Consider the matrix

$$\begin{array}{c} \\ b_1 \\ b_2 \\ b_3 \\ . \\ b_r \end{array} \begin{array}{c} \begin{array}{cccccc} c_1 & c_2 & c_3 & . & . & . & c_r \end{array} \\ \begin{bmatrix} m_{11} & 0 & 0 & . & . & . & 0 \\ m_{21} & m_{22} & 0 & . & . & . & 0 \\ m_{31} & m_{32} & m_{33} & . & . & . & 0 \\ . & . & . & . & . & . & . \\ m_{r1} & m_{r2} & m_{r3} & . & . & . & m_{rr} \end{bmatrix} \end{array} .$$

We observe that the determinant is not zero since each element of the principal diagonal is not zero. Thus, every finite subsystem of the set $b_1, b_2, \ldots,$ is independent, indicating that the entire set is also independent. We also assert that set $b_1, \ldots, b_n, \ldots$ form a basis of G. Suppose that there is a $g \in G$ which does not belong to $G' = \Sigma \{b_n\}$. Of all such g, pick one of least possible order and dependent on the set $\{c_1, \ldots, c_r\}$. Let $r = O(g)$. We have $mg = n_1c_1 + \ldots + n_rc_r$ for the same m as above. Put $n_r = qm_r + s$ $(0 \leq s < |m_r|)$; then from

$$mg = n_1c_1 + \ldots + n_rc_r \text{ and}$$

$$q(mb_r) = q(m_1c_1 + \ldots + m_rc_r), \text{ we have}$$

$$m(g - qb_r) = (n_1 - qm_1)c_r + \ldots + (n_r - qm_r(c_r.$$

Since b_r was chosen so as to give a minimal value $|m_r|$, it follows that $n_r - qm_r = 0$. Then either $g - qb_r = 0 \in G'$ or $g - qb_r$ depends on the set $\{c_1, \ldots, c_{r-1}\}$ so that $(g - qb_r)$ is in G', implying $g \in G'$, a contradiction.

For arbitrary groups we have

Theorem 1.18 Let $B = [a_\lambda]_{\lambda \in \Lambda}$ be a generating system of a group G consisting of elements of prime and/or infinite

order. B is a basis of G if and only if every finite subsystem $a_1, \ldots, a_k$ of B satisfies: $\{a_1, \ldots, a_k\} = \{b_1, \ldots, b_r\}$ with $O(b_i) = \infty$ or p^r implies

$$\min_{1 \leq i \leq k} O(b_i) \geq \min_{1 \leq i \leq k_1} O(a_i)$$

Proof: From Theorem 1.10, any two decompositions of a group G into direct sums of cyclic groups of order infinity and/or prime power are isomorphic. Thus, the necessity is clear. Conversely, suppose the system of orders $O(a_1), \ldots, O(a_k)$ is lexicographically the first of all such systems. Then $G = \{a_1\} + \ldots + \{a_k\}$. To prove this assertion, we show that the set of a_i are independent. Suppose the contrary; namely, that there is a relation $m_1a_1 + \ldots + m_ka_k = 0$ with $n_ia_i \neq 0$. Suppose that $\min O(a_i) = O(a_1)$ and assume $0 < m_1 < O(a_1)$. Set $m = (m_1, \ldots, m_k)$ (g.c.d.) and let $m_i = mn_i$. Then $(n_1, \ldots, n_k) = 1$ and by Lemma 1.5, we obtain $\{a_1, \ldots, a_k\} = \{b_1, \ldots, b_k\}$ where $b_1 = n_1a_1 + \ldots \ldots + n_ka_k$. Since $mb_1 = m_1a_1 + \ldots + m_ka_k = 0$ and $O(b_1) \leq m \leq m_1 < O(a_1)$, the arising contradiction completes the proof.

CHAPTER II

DIVISIBLE GROUPS

SECTION 1

THE CONCEPT OF DIVISIBILITY

In Chapter I, we considered groups which are the direct sums of cyclic groups. Another important class of groups is considered in the present chapter. Divisible groups play a role which is dual to free groups in a certain sense. As examples of this duality, every group is a homomorphic image of a free group while each group may be imbedded isomorphically in a divisible group. Free factor groups are isomorphic to direct summands while divisible subgroups prove to be direct summands.

Unlike groups which are direct sums of cyclic groups, divisible groups are easy to recognize and require no distinguished set of elements, like the basis, to decide the divisibility property. We offer several important and interesting properties characteristic of divisible groups.

We have defined multiplication of a group element by an integer. But what about division of an element by an integer? Unfortunately, this is not always possible and even when it is, the result need not be unique. In the event that an element $g \in G$ can be divided by an

integer n to yield again an element of G we say that g is divisible by n and denote this by n|g. Thus, n|g if there exists an element x ε G such that nx = g, or equivalently, if g ε nG.

A group G is divisible, if for every g ε G and every integer n, there is an element y ε G with ny = g; that is, if every element in G is divisible by every integer n. By a divisible subgroup we mean a subgroup which is divisible. In other words, for H to be a divisible subgroup of G, it has to be the case that for every h ε H and every integer n, there is an element k, again in H, satisfying nk = h.

The following are simple facts concerning divisibility

A) 0 is divisible by any integer n.

B) In the additive group of rationals, every element is divisible by every integer.

C) Cyclic groups and direct sums of cyclic groups are divisible.

D) Together with the solution x of the equation nx = g, the elements of the coset x + G[n] constitute the set of all solutions of the equation.

E) From part D) we conclude that if a group is torsion-free, then the quotient $n^{-1}g$ is unique, if it exists at all.

F) If the element g has order n, then g is divisible by every integer prime to n. To see this, let

$(n,m) = 1$; then there are integers s and t satisfying $ms + nt = 1$. Then $x = ts$ satisfies the relation

$$nx = ntg = 0 + ntg = msg + ntg = (ms + nt)g = g.$$

G) If $n|a$ and $n|b$, then $n|(sa + tb)$ for any integers s and t.

H) Suppose $pG = G$ for all primes p', then G is divisible. To verify this, we express n as a product of primes $n = p_1p_2\cdots p_r$. Then $nG = (p_1\cdots p_r)G = (p_1\cdots p_{r-1})(p_rG) = (p_1\cdots p_{r-1})G = \cdots = p_1G = G$. We have shown that a group is divisible if each of its elements is divisible by every prime.

I) Let G be a p-group. Then G is divisible if it satisfies the equation $pG = G$ for the single prime p. This statement is a consequence of part H) and part F) which implies $qG = G$ for primes $q \neq p$. We conclude that a p-group is divisible if and only if it contains no elements of zero height; i.e., if all of its elements are of infinite height.

J) If H is a homomorphic image of G, then $n|g$ $(g \varepsilon G)$ implies $n|h$ where h is the image of g under a homomorphism. The image y of x with $nx = g$ satisfies the equation $ny = h$.

Section 2

HOMOMORPHISMS INTO DIVISIBLE GROUPS

Let η be a homomorphism of a subgroup H of G into

a group K. We call a homomorphism x of the whole of G into K an extension of η to G if x has the same effect on the elements of H as does η ; i.e., if $a\eta = ax$ for every $a \in H$. A homomorphism of H into K need not have an extension to G, and if it does, the extension need not be unique.

Theorem 2.1 Let H be a subgroup of the group G. Let η be any homomorphism of H into a divisible group D. Then η can be extended to a homomorphism x of G into D.

Proof: Consider the subgroups U of G containing H, $H \subseteq U \subseteq G$ such that η has an extension Θ mapping U into D. The pairs $[U,\Theta]$ can be partially ordered by putting $[U,\Theta] \leqq [U',\Theta']$ if and only if U' contains U and the homomorphism Θ' mapping U' into D is an extension of Θ mapping U into D. In the partially ordered set of all pairs $[U,\Theta]$, every chain $[[U_\alpha,\Theta_\alpha]]_{\alpha\varepsilon}$ $\ldots \leqq [U_1,\Theta_1] \leqq \ldots \leqq [U_\alpha,\Theta_\alpha] \leqq \ldots$ has an upper bound $[U,\Theta]$; namely, $U = \bigcup_\alpha U_\alpha$ and Θ mapping U into D defined uniquely by $a\Theta = a\Theta_\alpha$ for $a \in U_\alpha$. Therefore, we may apply Zorn's Lemma to infer the existence of a maximal element $[U^*,\Theta^*]$ in the set of all $[U,\Theta]$. We show that $U^* = G$. Assume $U^* \subset G$ and let $g \in G$ with $g \notin U^*$. If g has nonzero multiples in U^*, then take $ng = \mu \in U^*$ with the least positive n and solve the equation $nx = \mu\Theta^*$ in D. We extend Θ^* from U^* to a homomorphism Θ^{**} of $[U^*,g]$ into D by putting $(a + tg)\Theta^{**} = a\Theta^* + tx$ with $a \in U^*$, $0 \leqq t < n$. $a + tg$ is the unique way of writing this element by our choice

of n and the requirement $t < n$. If no multiples of g other than $0.g = 0$ belongs to U*, then we define θ^{**} in the same way with an arbitrary $x \varepsilon D$ (now there is no restriction on t). θ^{**} is a homomorphism; for consider

$$[(a + tg) + (a' + t'g)]\theta^{**} = [(a + a') + (t + t')g]\theta^{**}$$

where $a, a' \varepsilon U^*$, and $t, t' < n$. Let $a + a' = a''$ and $t + t' = t''$; then we have

$$[a'' + t''g]\theta^{**} = a''\theta^{*} + t''x = (a + a')\theta^{*} + (t + t')x =$$

$$a\theta^{*} + tx + a'\theta^{*} + t'x = (a + tg)\theta^{**} + (a' + t'g)\theta^{**}.$$

We conclude $[U^*, \theta^*]$ is not maximal, a contradiction. Therefore, $U^* = G$ and $x = \theta^*$ is the desired extension.

Section 3

DIRECT SUMMAND PROPERTY

We may split from any group its divisible subgroups.

Theorem 2.2 If a divisible group D is a subgroup of some group G, then it is a direct summand of G.

Proof: Let D be a divisible subgroup of G. We wish to find a subgroup B with $D \cap B = 0$, $D + B = G$. Consider the set $E = \{\ldots, L_i, \ldots\}$ of all subgroups L which satisfy $D \cap L = 0$. There is at least one, namely 0. We would like to get an L as large as possible. Partially order the set E by set-theoretic inclusion. In order to apply Zorn's Lemma, we must verify that every chain in E has an upper bound. Suppose $\{L_i\}$ is a chain in E. To obtain the desired bound, take the set-theoretic union of

the L_i, say M. Three things must be verified. (a) M is a subgroup. We take x and y in M and show that $(x - y) \in M$. Now x and y get into M only because x is, say, in L_i, y in L_j. Also L_i and L_j are comparable, say $L_i \subseteq L_j$. Then both x and y are in L_j and since L_j is a subgroup, $x - y \in L_j$. Hence $x - y \in M$. (b) $D \cap M = O$. This follows from the fact that every element of M is in one of the L_i and for each L_i, $D \cap L_i = O$. (c) M is an upper bound of $\{L_1\}$. This is clear by construction.

Upon application of Zorn's Lemma, we obtain a maximal subgroup B in E; clearly $B \cap D = O$. We show that $D + B = G$. Suppose, to the contrary that there is an element, $x \in G$ such that $x \notin D + B$; then $x \notin B$. Form the subgroup B' generated by B and x. B' is larger than B and, in fact, B' consists of all elements $b + nx$ ($b \in B$, n an integer). By the maximality of B, we know that $D \cap B' \neq O$. Hence, there is a nonzero element $d = b + nx \in D \cap B'$. Since $nx = d - b$, we see that $nx \in D + B$. We have not yet used the divisibility of D. Thus, we have proved that if we take any subgroup H and a maximal subgroup K disjoint from H, then H + K is at any rate large enough so that $G/(H + K)$ is a torsion group. Suppose that n is the smallest positive integer such that $nx \in B + D$. Since $x \notin B + D$, we know that $n > 1$. Let p be a prime dividing n and write $y = (n/p)x$. Then $y \notin B + D$, but $py = nx = d - b$. By the divisibility of D,

Thus, we have proved that if we take any subgroup H and a maximal subgroup K disjoint from H, then H + K is at any rate large enough so that G/(H + K) is a torsion group. Suppose that n is the smallest positive integer such that $nx \in B + D$. Since $x \notin B + D$, we know that $n > 1$. Let p be a prime dividing n and write $y = (n/p)x$. Then $y \notin B + D$, but $py = nx = d - b$. By the divisibility of D, we may write $d = pd_1$ ($d_1 \in D$). Let $z = y - d_1$; then $z \notin B + D$, but $pz = py - pd_1 = d - b - pd_1 = d - b - d = -b \in B$, from $z = y - d_1$ $py = d - b$, and $pd_1 = d$. We now repeat the above argument with z in place of x. When we adjoin z to B we must obtain a subgroup not disjoint from D. Hence, we have $d_2 = b_2 + mz$ with m an integer, $b_2 \in B$, $d_2 \in D$, $d_2 \neq 0$. m is not a multiple of p, for if $m = np$, then $mz = n(pz) \in B$ since $pz \in B$, and $b_2 + mz \in B$, while $d_2 \in D$ and $d_2 \neq 0$. Hence, m is prime to p and there exist integers s and t such that $sm + tp = 1$. Then $z = smz + tpz \in B + D$ as seen by considering $d_2 = b_2 + mz$, $mz = d_2 - b_2$. Thus we have a contradiction.

A group is called <u>reduced</u> if it has no nonzero divisible subgroups.

<u>Lemma 2.3</u> Let D_λ ($\lambda \in \Lambda$) be a collection of divisible subgroups of some group G. Then $D = \{\ldots, D_\lambda, \ldots\}$ is divisible.

<u>Proof</u>: Let $g \in D$; then g has the form $g = g_1 + \ldots + g_k$ with $g_i \in D_{\lambda_i}$. For each i there is an element $x_i \in D_{\lambda_i}$

with $nx_i = g_i$, because each D_{λ_i} is divisible. Then $x = x_1 + \ldots + x_k$ belongs to D and satisfies $nx = g$.

Theorem 2.4 Any group G has a unique largest divisible subgroup M, and G = M + N, where N is a reduced group.

Proof: Let M be the subgroup generated by all of the divisible subgroups of G. M exists since the zero subgroup is divisible. By Lemma 2.3, M is divisible and also the maximal divisible subgroup of G. M is uniquely determined because it is intrinsically characterized as the maximal divisible subgroup. We note that N is unique up to isomorphism for N = G/M. By Theorem 2.2, M is a direct summand of G. The other summand N can have no divisible subgroups because any such would be divisible subgroups of G.

Section 4

A STRUCTURE THEOREM FOR DIVISIBLE GROUPS

Lemma 2.5 Let G be the direct sum of its subgroups, G_λ $(\lambda \varepsilon \Lambda)$; then G is divisible if and only if all of the G_λ are divisible.

Proof: The case in which G is the direct sum of two subgroups is given here. For the more general case in which G has three or more direct summands we have simply to modify the following remarks. Let G = A + B; then for any $g \varepsilon G$ we have $g = a + b$ $(a \varepsilon A, b \varepsilon B)$. If A and B are divisible, then A + B is divisible by Lemma 2.3. Suppose

that A + B is divisible. Let a ε A; for any positive integer m, there exists an x ε A + B such that mx = a. Since G = A + B, x = a' + b' (a' ε A, b' ε B). Then a = mx = ma' + mb'. By the uniqueness of the decomposition into direct sums for any group, we have a = ma'.

As examples of divisible groups, we have

(a) The quasicyclic group, $\mathcal{C}(p^\infty)$. For a fixed prime p, $\mathcal{C}(p^\infty)$ contains, as subgroups, finite cyclic groups of all orders p^n (n = 1, 2, ...) but no proper subgroup of it has this property. Since $\mathcal{C}(p^\infty)$ is a p-group, all of its elements are divisible by any integer prime to p. On the other hand, every element of $\mathcal{C}(p^\infty)$ can be divided by arbitrary powers of p.

(b) The additive group of rationals, $\mathcal{R}$. Every element of $\mathcal{R}$ is divisible by every nonzero integer.

To classify all groups it is enough, by Theorem 2.4, to consider the divisible and reduced cases. As a consequence of Lemma 2.5, we have that any direct sum of groups $\mathcal{C}(p^\infty)$ and $\mathcal{R}$ is again a divisible group. Theorem 2.6 asserts there are no other divisible groups.

Theorem 2.6 A diviisible group is a direct sum of quasicyclic and full rational groups. Any two such decompositions are isomorphic.

Proof: Let G be a divisible group and T its maximal torsion subgroup. Then T must again be divisible since for x ε T there is an integer m ∋ mx = 0 (x is a torsion element).

By the divisibility of G, for an integer n, there is a $y \in G$ such that $ny = x$. Then $mny = mx = 0$, indicating y also belongs to T. Theorem 2.2 implies that $G = T + F$ where F is torsion-free since T is a maximal torsion subgroup. By Lemma 2.5, we conclude F is a divisible subgroup since it is a direct summand of the divisible group G. Similarly, since T is a torsion group, it can be expressed as a direct sum of p-groups, and, because it is divisible, each of its p-components T_p is again divisible. We show that T_p is a direct sum of groups $\mathcal{C}(p^\infty)$ and F is a direct sum of groups $\mathcal{Q}$.

First consider T_p and select a maximal independent set $[a_\lambda]_{\lambda \in \Lambda}$ in the socle of T_p. Owing to the divisibility of T_p, for each λ we can find an infinite sequence $a_{\lambda 1}, \cdots, a_{\lambda n}, \cdots$ with $a_{\lambda 1} = a_\lambda$, $pa_{\lambda 2} = a_{\lambda 1}, \cdots$, $pa_{\lambda(n+1)} = a_{\lambda n}, \cdots$. It follows that every a_λ may be imbedded in a quasicyclic subgroup Q_λ of T_p generated by $a_{\lambda 1}, \cdots, a_{\lambda n}, \cdots$. Since $\{a_\lambda\}$ is the socle of Q_λ, and $[a_\lambda]_{\lambda \in \Lambda}$ is an independent set, the Q_λ generates the direct sum $Q = \sum_{\lambda \in \Lambda} Q_\lambda$ in T_p. To see that $Q = T_p$, observe that Q, as a divisible subgroup, is a direct summand of T_p, $T_p = Q + S_p$. But Q contains a maximal independent set of the socle of T_p; hence, $S_p = 0$ and $Q = T_p$.

Proceeding to F, select a maximal independent set $[b_\mu]_{\mu \in M}$ in F. By the divisibility and torsion-free properties of F and by (E) of section 1 of Chapter II, there

is just one element x in F with nx = b; because if nx = b and ny = b, then n(x - y) = 0 which contradicts the torsion-free character of F. Thus each $\{b_\mu\}$ may be extended to a full rational group B_μ of F as the additive integers may be extended to the rationals. By the independence of the b_μ, the groups B_μ generate the direct sum $B = \sum_{\mu \in M} B_\mu$. By Theorem 2.2, B is a direct summand of F. To see that B = F, observe that B, as a divisible subgroup, is a direct summand of F, F = B + U. But B contains a maximal independent set of F so U = 0.

To prove uniqueness, we remark that if we single out from each $\mathcal{C}(p^\infty)$ and $\mathcal{R}$ some nonzero element, we obtain a maximal independent set. If we let r(G) be the cardinal number of a maximal independent system in G, then all we need do is to appeal to the uniqueness of the ranks, $r_p(G)$ and $r_o(G)$ to obtain the desired result.

As a consequence of Theorem 2.6, every maximal independent system consisting of elements of infinite and/or prime power order gives rise to a decomposition of the divisible group into the direct sum of full rational and quasicyclic groups. The next result asserts that the problem of describing all groups is the same as that of the enumeration of the subgroups of divisible groups.

Theorem 2.7 Every group can be imbedded in a divisible group.

Proof: An infinite cyclic group can be imbedded in a full

rational group, just as the integers can be imbedded in the rationals. Hence, every free-group is a subgroup of a (torsion-free) divisible group. But any group G is a factor group F/N of a free-group F and we may embed F in a divisible group D. Then G is isomorphic to the subgroup F/N of the divisible group D/N.

Section 5

GROUPS WITH MINIMUM CONDITIONS

A group G is said to satisfy the minimum condition, if every descending chain of distinct subgroups $A_1 \supset A_2 \supset \ldots$ is necessarily finite.

Theorem 2.8 The collection of all subgroups of G satisfy the minimum condition if and only if G is a direct sum of a finite number of quasicyclic and/or cyclic p-group.

Proof: Let the subgroups of G satisfy the minimum condition. G has no elements of infinite order because an element a of infinite order produces the infinite descending chain $\{a\} \supset \{2a\} \supset \{4a\} \supset \ldots$. To see that G has but a finite number of p- components G_p, consider the subgroup F' of G generated by the p-components of G; $G' = \sum_{\lambda \in \Lambda} G_\lambda$ (Λ is a subset of the set of primes). Let $\Lambda = \{\lambda_1, \lambda_2, \ldots\}$. Then consider the sequence

$$G' \supset \sum_{\lambda \in \Lambda - \{\lambda_1\}} G_\lambda \supset \sum_{\lambda \in \Lambda - \{\lambda_1, \lambda_2\}} G \supset \ldots .$$

It is a properly descending chain. The rank of G_p is finite,

for otherwise $F_p[p]$ would be the direct sum of infinitely many $\mathcal{C}(p)$, contradicting the minimum condition as above. Let $A_p = p^m G_p$ be a minimal member of the descending chain, $p^k G_p$ $(k = 1, 2, \ldots)$; then $pA_p = p^{m+1} G_p = p^m G_p = A_p$ is divisible. We have used the definition: S is divisible if $nS = S$ for each integer n. By Theorem 2.2, G_p is a direct sum $A_p + B_p$ where $p^m B_p = 0$ because $p^m G_p = p^m A_p + p^m B_p = A_p$. The finiteness of the rank implies that B_p is finite; consequently, by Theorem 2.6, G_p is a direct sum of a finite number of quasicyclic and cyclic p-groups.

Conversely, if G_p is the direct sum of a finite number of quasicyclic and/or cyclic p-groups, then its subgroups satisfy the minimum condition. If $r(G_p) = 1$, then the only subgroups of G_p are in the sequence $\mathcal{C}(p^k)$ $(1 \leq k \leq \infty)$ and the statement follows For $r(G_p) = r > 1$ we use induction and assume our assertion true for groups of rank $\leq r - 1$. Put $G_p = H + \mathcal{C}(p^k)$ and let $K_1 \supseteq K_2 \supseteq \ldots$ be a descending chain in G_p. Then $H \cap K_1 \supseteq H \cap K_2 \supseteq \ldots$, and from some index r on we must have $H \cap K_r = H \cap K_{r+1} = \ldots$. Since $K_i/(H \cap K_r) = K_i/(H \cap K_i) \cong \{H, K_i\}/H \subseteq G/H \cong \mathcal{C}(p^k)$ with $i \geq r$, we infer that the $K_i/(H \cap K_r)$ and therefore the K_i as well are equal from some index on.

CHAPTER III

DIRECT SUMMANDS AND PURE SUBGROUPS

Section 1

INTRODUCTION

The groups mentioned so far have had a very special property; they decompose into the direct sum of cyclic or quasicyclic and full rational groups. Although most groups cannot be so decomposed, many groups can be written as the direct sum of two of their subgroups, one of which has rather special properties. If a group G is the direct sum of two of its subgroups A and B, then B is called a complement of A in G. In general, B is determined only up to isomorphism by A. In Chapter II we found that a divisible group D is not only a direct summand of every group G containing it but also every subgroup of G disjoint from D can be extended to a complement of D. Our present purpose is to determine which direct summands of a group have the same property.

A subgroup A of a group G is called an absolute direct summand of G if for every subgroup B of G which is maximal with respect to the property $M \cap H = 0$, one has $G = A + B$.

Lemma 3.1 Let H be a subgroup of a group G and M a subgroup of G maximal with respect to the property $M \cap H = 0$.

Then $G^* = H + M$ has the following properties: (i) G/G^* is a torsion group and (ii) $(G/G^*)[p] = (\{pG,M\} \cap H)/pH$.

Proof: In order to verify (i) we appeal to the proof of Theorem 2.2 and, in particular, to the remark interpolated into the proof. To verify (ii), observe that all of the nonzero elements of both groups in question are of order p, since, by definition, $(G/G^*[p]$ consists of all elements $g \in G/G^*$ with $pg = 0$, and p times any element in $\{pG,M\} \cap H$ is in pH. Denote $\{pG,M\} \cap H$ by H_1. Take $x^* \in (G/G^*)[p]$ and select some $x \in x^* = x + G^*$, then $px^* = px + pG^*$. But $px^* = 0$, and so $px \in pG^*$ and from $G^* = H + M$, we have $px = h + b$ $(h \in H, b \in M)$ and $h = px - b \in H_1$. Consider the correspondence η mapping x^* on $h^* = h + pH$. Let x_1 and x_2 be representatives of the same coset x^*. Then from $px_1 = h_1 + b_1$, $px_2 = h_2 + b_2$ and from the fact that x_1 and x_2 are from the same coset x^*, we have $x_1 - x_2 = h_3 + b_3$ $(h_i \in H, b_i \in M)$. We conclude $ph_3 + pb_3 = px_1 - px_2 = (h_1 + b_1) - (h_2 + b_2) = (_1 - h_2) + (b_1 - b_2)$ or, since $H \cap M = 0$, $h_1 - h_2 = ph_3$. Finally, $h_1^* = h_2^*$ and so η is single-valued. Under η all of H_1/pH is exhausted. If $h \in H_1$ but $h \notin pH$, then $h = py - b$ $(y \in G, b \in M)$ and here $y \notin G^*$ because $y = h' + b'$ $(h' \in H, b' \in M)$ would imply $py = ph' + pb' = h + b$, $h = ph' \in pH$. Thus, y^* is mapped upon h^* under η.

η^{-1} is single valued. Let both x_1^* and x_2^* be mapped by η upon the same h^*. As above, we have

$px_1 = h_1 + b_1$, $px_2 = h_2 + b_2$, $h_1 - h_2 = ph_3$ ($h_i \in H$, $b_i \in M$). Set $w = x_1 - x_2 - h_3$. In case $w \in M$, we have $x_1 - x_2 \in H + M = G^*$ and we are finished. In case $w \notin M$, there is a nonzero $z = b + kw \in \{M,w\} \cap H$ where because of $pq = px_1 - px_2 - ph_3 = h_1 + b_1 - b_2 - h_2 - h_1 + h_2 = b_1 - b_2 \in M$, we must have $(k,p) = 1$. From $z = b + kw$, we have $kw = z - b \in G^*$ since $z \in \{M,w\} \cap H$ and thus, $z \in H$ while $b \in M$. Considering $kw \in G^*$ and $pw \in M$, we conclude $w \in G^*$. The last result is obtained as follows: $(k,p) = 1$, there are integers m and n such that $mk + np = 1$ and thus, $w = nkw + npw$. Now $kmw \in G^*$, $pnw \in M$. It follows that $x_1 - x_2 \in G^*$ and $x_1^* = x_2^*$. The correspondence η is, therefore, one-to-one between $(G/G^*)[p]$ and H_1/pH.

η carries sums into sums. Let η map x_1^* into h_1^*, x_2^* into h_2^*, and suppose x_1 is a representative of x_1^*, x_2 of x_2^*, h_1 of h_1^*, and h_2 of h_2^*. From $px_1 = h_1 + b_1$, $px_2 = h_2 + b_2$, we have $p(x_1 + x_2) = h_1 + h_2 + b_1 + b_2$, from which we have the desired result.

Two consequences of Lemma 3.1 are

(a) If H is divisible, H is an absolute direct summand. Indeed $pH = H$ for every prime p implies that the p-socle of the torsion group G/G^* vanishes and so $G^* = G$.

(b) If the elements of G are of bounded order and $a \in G$ is an element of maximal order p^k, then for $H = \{a\}$ we have,

if $H_1 = \{pG, M\} \cap H$, $p^{k-1}H_1 \subseteq \{p^kG, p^{k-1}M\} \cap p^{k-1}H = p^{k-1}M \cap p^{k-1}H = 0$. Hence $H_1 \subseteq \{pa\} = pH$ and the lemma implies that $\{a\}$ is a direct summand of G. (Lemma 1.3)

Theorem 3.2 A direct summand A of G is an absolute direct summand if and only if one of the following holds: (i) A is divisible; (ii) G/A is a torsion group and $p^t(G/A)_p = 0$ whenever there is an element in A, not in pA, whose order is p^t. (We denote by H_p the p-component of the maximal torsion subgroup of H).

Proof: Let A be an absolute direct summand of G which is not divisible. Since A is not divisible ($\exists A \neq A$), there is a prime p and an element, $a \in A \ni a \in pA$. We show that if $b \in B$ and $u = a - pb$, then $\{u\} \cap A \neq 0$. To see this, observe that if the intersection were empty we could choose an M with $u \in M$ and maximal with respect to the property $M \cap A = 0$. But then $a = pb + u \in A \cap \{pG, M\} = A_1$, $a \notin pA$ Would imply, in view of Lemma 3.1, that $A + M \subset G$ contradicting the hypothesis on A, for A was chosen to be an absolute direct summand and M was chosen maximal with respect to the property $M \cap A = 0$ from which we should have $G = A + M$. Thus some nonzero multiple of u is a nonzero element of A. Consequently, for some integer n we have $nu \in A$; i.e., $na - npb \in A$. But $npb \in B$ and $A \cap B = 0$, so $npb = 0$ while $na \neq 0$. Thus, the order of b cannot be infinite and G/A is a torsion group because b is arbitrary in B, b has finite order, and $B = G/A$. If $a \in A_p$, $O(a) = p^t$, $b \in B_p$, then

$p^{t-1}a \neq 0$ and $p^t b = 0$. Hence, $p^t B_p = 0$.

Let A be divisible and therefore a direct summand of G. Let B be a complement of A. Suppose $B = G/A$ satisfies ii), and that $A + M \subset G$ for some M maximal with respect to the property $M \cap A = 0$. By Lemma 3.1, this means that for some prime p we have $A_1 = \{pG, M\} \cap A \supset pA$; i.e., there is an $a = pg + c \in A$ ($g \in G$, $c \in M$) with $a \notin pA$. We may assume $g \in B$. By ii), g is of a finite order $p^t s$ with $(p,s) = 1$. Since we have again $sa = p(sg) + sc \in A_1$, $sa \notin pA$, there is no loss in generality in supposing $O(g) = p^t$. Surely, $t \geq 2$, because $a = c \in M$ cannot hold. Then $p^{t-1}a = p^{t-1}c$ so $p^{t-1}a = 0$, $O(a) < O(g)$ contradicting ii).

Section 2

PURE SUBGROUPS

It may happen that $n|a$ holds in a group G but not in a subgroup H of G containing a. Those subgroups S for which $n|a$ in S means the same as $n|a$ in G play a distinguished role in the theory of groups. A subgroup S of G is called a pure subgroup of G if the equation $nx = g \in S$ is solvable in S whenever it has a solution in G. In other words, if an element of S is divisible by n in G, it is already divisible by n in S. We express purity in the form of an equation: S is pure if and only if $nS = S \cap nG$ for every positive integer n. That these two definitions are equivalent can be seen by observing the inclusion $nS \subset S \cap nG$ is

true for every subgroup S of G and thus, the essential requirement is $nS \supseteq S \cap nG$; i.e., each element of S which may be written as n times some element of G is n times some element of S. This is actually nothing else than purity.

Theorem 3.3 Let S be a subgroup of a group G such that S is a direct sum of cyclic groups of the same order p^k. Then the following statements are equivalent: (i) S is a direct summand of G; (ii) S is a pure subgroup of G; (iii) S satisfies $p^kG \cap S = 0$.

Proof: We will show, in turn, that first, (i) implies (ii). Any direct summand is pure; for suppose $G = S + T$, that $x \in S$ and that $x = ny$ with $y \in S$. Then $s = ny_1$ where y_1 is the component of y in S. Thus, S is pure. Next, (ii) implies (iii). If S is a pure subgroup of G, then we have $p^rG \cap S = p^rS$ for every positive integer r, from the definition. In particular, for $r = k$ when $p^kS = 0$ holds. Finally, (iii) implies (i). Let M be a subgroup of G maximal with respect to the properties $p^kG \subseteq M$ and $M \cap S = 0$. Then M and S generate their direct sum $G' = M + S$. Assume the existence of an element $g \in G$ such that $g \notin G'$, $pg \in G'$. Multiplying $pg = a + b$ ($a \in M$, $b \in S$), by p^{k-1} we obtain $p^kg = p^{k-1}a + p^{k-1}b$ so that $p^{k-1}b = 0$ because $p^kG \subseteq M$. The assumption on S guarantees the existence of a $c \in S$ with $pc = b$. Then $h = g - c$ satisfies $h \notin G'$, $ph \in M$. Consequently, there is a nonzero element $d + kh$ ($d \in M$) in the intersection

$\{M,h\} \cap S$ where $(k,p) = 1$. To see that $(k,p) = 1$, observe that $ph \in M$ so that if $k = np$, then $kh = nph \in M$; but $M \cap S = 0$. Now h was picked so that it does not belong to G' but we show that the three statements $(p,k) = 1$, $kh \in M + S$, and $ph \in G'$ lead us to the contradiction $h \in G'$. From $(k,p) = 1$, we have $1 = pt + ks$ for integers t and s. Then $h = pth + ksh$ where pth and ksh belong to G' and so $h \in G'$.

Corollary 3.4 Every element a of order p and of finite height can be imbedded in a finite direct summand.

Proof: Let a be an element of a group G such that the order of a is p and the height of a is r - 1. Choose $a, b \in G$ such that $p^{r-1}b = a$ so that height of b is zero. Denote by K the subgroup $\{b\}$ of G generated by the element b. K is a pure subgroup of G containing a; and, by Theorem 3.3, K is a direct summand of G. $O(b) = p^r$ since $p(p^{r-1}b) = pa = 0$. Recall that in a p-group every element is automatically divisible by every integer prime to p. Thus we confine our attention to powers of p. Suppose that $p^ib = p^jy$ for $i < r$ and some $y \in G$. We show that p^ib is divisible by p^j within K. If $j \leq i$, the assertion is clear. If $j > i$, we have $a = p^{r-i-1}(p^ib) = p^{r-i-1}(p^jy) = p^{r-1+(j-i)}y$, from which we conclude the height of a is greater than r - 1 since $j - i > 0$. Thus, we have a contradiction since, by hypothesis, the height of a is r - 1.

A second corollary to Theorem 3.3 asserts that a

non-divisible torsion group has a non-cyclic direct summand. For the proof of this Corollary 3.6, we make use of a lemma which is interesting in its own right.

Lemma 3.5 If, in a p-group G, every element of order p is of infinite height, then G is divisible.

Proof: Let $a \in G$. If $E(a) = 1$; i.e., $pa = 0$; then, by hypothesis, p divides a. Applying an inductive argument, suppose we have proved the divisibility of the elements of G by p for elements with exponent less $E(a) = k > 1$. Since $p^{k-1}a$ is of infinite height, there is a $b \in G$ such that $p^k b = p^{k-1}a$, from which we obtain $p^{k-1}(a - bp) = 0$. Now $(a - pb)$ is of a smaller order than a and so, by our inductive hypothesis, $(a - -b)$ is divisible by p; i.e., for some $y \in G$ we have $py = a - pb$, from which we obtain $p(y + b) = a$ with $(y + b) \in G$. Thus, $p|a$.

Corollary 3.6 If a group contains elements of finite order, then it has a direct summand of the form $\mathcal{C}(p^k)$ $(1 \leqq k \leqq \infty)$ for some prime p.

Proof: If G contains a subgroup $\mathcal{C}(p^\infty)$ for some prime p, then $\mathcal{C}(p^\infty)$ is a divisible subgroup of the group G and as such is a direct summand. If G contains no subgroup $\mathcal{C}(p^\infty)$ but contains elements of order p, then these elements belong to a subgroup A contained in the maximal torsion subgroup of G. (By Theorem 0.2, A is a p-group). If G were divisible, then by Theorem 2.6, $A \supseteq \mathcal{C}(p^\infty)$, contradicting our assumption. Applying Lemma 3.5 to our

conclusion that G is not divisible, we infer the existence of an element a of order p and of finite height. Corollary 3.4 then yields the result.

In Theorem 3.3, we found that every direct summand is a pure subgroup. We now state and prove another property of pure subgroups.

Lemma 3.7 Purity is a transitive property; i.e., if S is a pure subgroup of a group G and if T is a pure subgroup of S, then T is a pure subgroup of G.

Proof: For every integer n we have

$$nT = T \cap nS = T \cap (S \cap nG) = (T \cap S) \cap nG = T \cap nG.$$

From our definition of purity, T is pure in G.

Theorem 3.8 Let S be a bounded, pure subgroup of a group G. Then S is a direct summand of G.

Proof: By Theorem 1.8, a bounded group S may be written in the form $S = S_1 + T$ where S_1 is a direct sum of cyclic groups of the same order p^k, and the least upper bound of the orders of the elements in T is smaller than that of S_1. If S is a pure subgroup in G, then by Theorem 3.3 and Lemma 3.7, S_1 is again pure in G, and $G = S_1 + G_1$. Hence, $S = S_1 + T_1$ where $T_1 = S \cap G_1 \cong T$. Since T_1 is a direct summand of the pure subgroup S, T_1 is a pure subgroup of S. Also $T_1 = S \cap G_1$ so we conclude T_1 is a pure subgroup of G_1. Also T_1 has bounded order. We apply an inductive argument on n. Assume the theorem true for pure subgroups of bounded order such that the least upper bound of their

orders is less than the least upper bound of the orders in S. By the inductive hypothesis, it follows that T_1 is a direct summand of G_1, say, $G_1 = T_1 + H$. Then S is a direct summand of G since

$$G = S_1 + G_1 = S_1 + (T_1 + H) = (S_1 + T_1) + H = S + H.$$

Corollary 3.9 A finitepure subgroup is a direct summand.

Theorem 3.10 A p-group A of a group G can be imbedded in a bounded direct summand of G if and only if the height of the elements of A (taken in G) are bounded.

Proof: Let the p-subgroup A of G be imbedded in a bounded direct summand S. Then the heights of the elements of A are bounded. (In fact the heights of the elements of S are bounded). Since S is a bounded direct summand for some integer n, we have $p^nS = 0$. Then for any element $x \in A$, since $A \subseteq S$, we have $x \notin p^nS$ if $x \neq 0$. Conversely, if k is the l.u.b. of the heights of A, then pick in G a subgroup H maximal with respect to the properties $A \subseteq H$, $H \cap p^{k+1}G = 0$, by applying Zorn's Lemma. Then H is a bounded subgroup. For suppose H is not bounded; then $p^rH \neq 0$ for all r. In particular, $p^{k+1}H \neq 0$. But then $0 \neq p^{k+1}H \subseteq H \cap p^{k+1}G = 0$, a contradiction. H is pure in G; i.e., $H \cap p_nG \subseteq p_nH$ for nonnegative integers n. The inclusion is clear for $n = 0$ and we apply induction on n. Let $h = p^{n+1}g$ ($h \in H$, $g \in G$). If $p^ng \in H$, then $p^ng \in H \cap p^nG \subseteq p^nH$ by our inductive hypothesis; therefore $h = p(p^ng) \in p^{n+1}H$. If $p^ng \notin H$, then $n \leq k$ because, in any case, $p(p^ng) \in H$ and if $n = k$ we have $p(p^ng) \in p^{k+1}G$.

Since $H \cap p^{k+1}G = 0$, we have $pg = 0$ for all $n > k$. Thus, by the maximality of H, there is a nonzero element $rp^n g + h'$ (r an integer, $h' \in H$) in the intersection $\{H, p^n g\} \cap p^{k+1}G$ where again $(r,p) = 1$. Now $n \leq k$ implies $h' \in H \cap p^n G$; thus, $h' \in p^n H$ by our inductive hypothesis. From $p(rp^n g + h') = rh + ph' \in H \cap p^{k+1}G = 0$ we obtain $rh = -ph' \in p^{n+1}H$, $h \in p^{n+1}H$ (from $(r,p) = 1$). Consequently, H is a bounded, pure subgroup in G, and so, by Theorem 3.8, H is a direct summand of G.

Remark: In the proof of Theorem 3.10 there is a proof of: "If A is a p-subgroup of G the heights of whose elements (taken in G) are bounded, then A may be imbedded in a bounded, pure subgroup of G".

Theorem 3.11 An element a of prime power order is contained in a finite direct summand of G if and only if, $\{a\}$ contains no elements of infinite height.

Proof: (Since the statement does not involve elements of infinite order and it holds for a if it holds for the generators of the p-component of $\{a\}$, we restrict our attention to elements of prime power order.) The necessity is like the necessity portion of the proof of Theorem 3.10. For the sufficiency, suppose the element a is of prime power order and that $\{a\}$ contains no elements of infinite height. Then a is contained in a finite direct summand of G. This assertion follows from the proof of Theorem 3.10 by noting $A = \{a\}$, imbedding A in a bounded direct summand

H of G and then selecting in H a finite direct summand containing a.

Lemma 3.12 If S is a pure subgroup of G and T is a subgroup of S, then S/T is pure in G/T.

Proof: Suppose $n(g + T) = a + T$ ($a \in S$, $g \in G$, n an integer). Then $ng = a + b \in S$ ($b \in T$) because $a \in S$ and $T \subseteq S$. From our hypothesis, it follows that there is an element $c \in S$ with $nc = a + b$, so that $n(c + T) = nc + nT = a + (b + nT) = a + T$.

Section 3

FACTOR GROUPS WITH RESPECT TO PURE SUBGROUPS

In section 2 we considered conditions which insure the direct summand property of certain pure subgroups. We consider in this section the same kind of problem but the conditions to be considered will apply to properties of factor groups with respect to pure subgroups rather than the structure of the pure subgroups themselves. First, a characterization of pure subgroups:

Theorem 3.14 Let S be a pure subgroup of a group G. Consider the natural homomorphism $\nu: G \to G/S$. The purity of S insures the possibility of selecting in each coset of G an element having the same order as this coset.

Proof: If the particular coset has infinite order, then any choice of an element of G mapping onto it will do. Suppose y is any coset in G/S with finite order n. Choose

any $x \in G$ mapping on y, then $nx \in S$. By the purity of S, there is an element $h \in S$ with $nx = nh$. Set $w = x - h$. Then w has the desired properties: it maps on y and has order n.

Theorem 3.15 Let G be a group and S a pure subgroup such that G/S is a direct sum of cyclic groups. Then S is a direct summand of G.

Proof: For each cyclic summand of G/S pick a generator y_i. By Theorem 3.14, we select elements $x_i \in G$ which are mapped by the natural homomorphism onto the coset y_i and have the same order as y_i. (We have again made use of the Axiom of Choice). Let K be the subgroup of G generated by the elements x_i; then $G = S + K$. To justify this claim we prove (a) $S + K = G$, and (b) $S \cap K = 0$.

(a) $S + K = G$. Let t be any element in G, mapping, let us say, on $t^* \in G/S$. We may write t^* as a finite sum $a_1y_1 + \ldots + a_ky_k$ with integral coefficients. Then $t - (a_1x_1 + \ldots + a_kx_k)$ maps on 0 in G/S and so lies in S. Since $(a_1x_1 + \ldots + a_kx_k) \in K$, we have $t \in S + K$.

(b) $S \cap K = 0$. Let $w \in S \cap K$, say $w = a_1x_1 + \ldots + a_kx_k$. Since $w \in S$, we have $(a_1y_1 + \ldots + a_ky_k) = 0$. If y_i has infinite order, this means $a_i = 0$; if y_i has finite order n_i, then a_i must be a multiple of n_i. In either case, $a_ix_i = 0$ for each i, and $w = 0$. Theorem 3.14 was needed to insure elements of the proper order.

Corollary 3.16 If S is a pure subgroup of a group G and

G/S is finitely generated, then S is a direct summand of G.

Proof: By Theorem 1.6, a finitely generated group is the direct sum of a finite number of cyclic groups of infinite and/or prime power order. Then our hypothesis implies that G/S is a direct sum of cyclic groups and so the statement is a consequence of Theorem 3.15.

CHAPTER IV

BASIC SUBGROUPS

Section 1

INTRODUCTION

In the study of groups, many p-groups cannot be decomposed into the direct sum of cyclic groups, even in the case in which the p-groups are free of elements of infinite height. There are p-groups without basis. In this chapter we consider a concept which may be thought of as a substitute for the basis, in case the p-group has no basis. The notion of a basic subgroup of a p-group is fundamental to the theory of groups of arbitrary power.

A subset $[x_\lambda]_{\lambda \in \Lambda}$ of a group G is called pure independent if it is an independent set and generates a pure subgroup of G; i.e., if $\{\ldots, x_\lambda, \ldots\} = \sum_{\lambda \in \Lambda} \{x_\lambda\}$ is a pure subgroup of G. That G contains maximal pure independent subsets and that a pure independent subset can be extended to a maximal one are applications of Zorn's Lemma.

Lemma 4.1 If T is a pure subgroup of G and S/T is a pure subgroup of G/T , then S is pure in G.

Proof: Let $ng = a$ ($a \in S$, $g \in G$, $n \in I$); then $n(g + T) = a + T$ and by hypothesis there is some $b \in S$ such that $n(b + T) = a + T$. Now $nb = a + u$ ($u \in T$) so that $n(b - g) =$

u and, by the purity of T, we have $n(b - g) = nv$ $(v \in T)$. This gives $n(b - v) = ng = a$ where $(b - v) \in S$.

Lemma 4.2 The pure independent subset $L = [a_\lambda]_{\lambda \in \Lambda}$ of the p-group G is maximal if and only if the factor group $G/\{L\}$ is divisible.

Proof: Assume L is a maximal pure independent set in G and let $B = \{L\}$. We show that the factor group G/B is divisible Corollary 3.6 asserts that a non-divisible torsion group has a nonzero cyclic direct summand and so it is enough to show that G/B has no nonzero cyclic direct summands. Suppose G/B has such a direct summand $\{c^*\}$, then consider the corresponding subgroup C of G, $C/B = \{c^*\}$. By Corollary 3.16, $C = B + \{c\}$ where $c \in c^*$. Lemma 4.1 implies C is pure in G. Thus [L,c] would be a larger pure independent set - contradicting the maximality of L.

Conversely, if G/B is divisible, then any enlarged independent set $L' = [L,c]$ is no longer pure because $px = b + c$ is solvable in G for some $b \in B$, but admits no solution in $1' = B + \{c\}$. Suppose $x \in G/B$, $x = d + B$ $(d \in G)$; then $d + B$ is a solution of $px = c + B$. For $px = c + B$ we have $p(d + B) = c + B$, and then $pd = c + b$ for some $b \in B$. Also $px = b + c$ is not solvable in L' because x can be written in the form $x = m_1 a_{\lambda_1} + \ldots + m_r a_{\lambda_r} + mc$ $(a_{\lambda_i} \in B,\ c \in \{c\},\ m, m_i \in I)$. Then $p(m_1 a_{\lambda_1} + \ldots + m_r a_{\lambda_r} + mc) = b + c$. But this implies that c is dependent on the set B, contradicting the independence

of the set [L,c].

A subgroup B of a p-group G is called a basic subgroup if it satisfies the conditions: (i) B is a direct sum of cyclic groups; (ii) B is pure in G; (iii) G/B is divisible.

Theorem 4.3 Every p-group contains a basic subgroup B.

Proof: Let B be a subgroup generated by a maximal pure independent set of G. The existence of such a maximal set may be proved by an application of Zorn's Lemma. Then (i) follows from the fact that B is generated by an independent set, (ii) follows from the fact that B is generated by a pure independent set, and finally (iii) is an immediate consequence of Lemma 4.2 - We remark that a group may have several basic subgroups.

For each n, let B be the direct sum of those direct summands of B of the form $\mathcal{C}(p^n)$. Then

(1) $\quad B = B_1 + B_2 + \ldots + B_n + \ldots \quad (B_n = \Sigma\, \mathcal{C}(p^n))$.

For each n, $B_1 + \ldots + B_n$ is pure in G and since it is a bounded group (with bound p^n), it is, in view of Theorem 3.8, a direct summand of G, so that we may write

(2) $\quad G = B_1 + \ldots + B_n + G_n$.

We will show that the complementary direct summand G_n may be chosen such that $G_n = B_{n+1} + B_{n+2} + \ldots, p^nG$. (Then we shall have $G_n \geq G_{n+1}$). Moreover,

Theorem 4.4 Assume B is a subgroup of the p-group G and $B = \sum_1^\infty B_n$ where B_n is a direct sum of cyclic groups of order

p^n. Then B is a basic subgroup of G if and only if

(3) $\quad G = B_1 + \ldots + B_n + \{B_n^*, p^nG\}$ for every n

where $B_n^* = B_{n+1} + B_{n+2} + \ldots$.

Proof: We show that a basic subgroup B satisfies (3). Every element $g \in G$ may be written by virtue of part (iii) of the definition of basic subgroups in the form $g = b + p^nx$ $(b \in B, x \in G)$ showing that $B_1, \ldots, B_n$ and B_n^*, p^nG together generate G. We note the intersection $\{B_1 + \ldots + B_n\} \cap \{B_n^*, p^nG\}$ is empty. If $g \in B_1 + \ldots + B_n$ and $g \in \{B_n^*, p^nG\}$, then $g = b + p^nx$ $(b \in B_n^*, x \in G)$ belongs to $B_1 + \ldots + B_n$ implying that $p^nx \in B$. Moreover, $p^nx \in B_n^*$ as we now show. Observe first that $p_nx \in B$, a pure subgroup. Using the purity of B, we have $p_nx = p_ny$ $(y \in B)$. Using the direct summand property, $y = b + b^*$ $(b \in B_1 + \ldots + B_n$ $b^* \in B_n^*)$, $p^ny = p^nb + p^nb^* = 0 + p^nb^*$, and hence, $p^nx = p^nb^*$ with $b^* \in B_n^*$ so that $p^nx \in B_n^*$. Thus, g is an element common to both $B_1 + \ldots + B_n$ and B_n^*; hence, $g = 0$.

Conversely, let $B = \Sigma B_n$ satisfy (3). Then B is a direct sum of cyclic groups and is pure as the union of the tower of direct summands $B_1 + \ldots + B_n$ of G. B6 (3), every $g \in G$ may be written in the form $g = b + c + p^nx$ $(b \in B_1 + \ldots + B_n, c \in B_n^*, x \in G)$. Hence, $p^nx \equiv g \pmod{B}$ is solvable for every n and thus, G/B is divisible. This proves that B is a basic subgroup of G.

By an m-bounded direct summand of G, we mean a direct

summand of G in which the elements are all of order $\leq m$.

Theorem 4.5 Suppose B is a subgroup of the p-group G and $B = \sum_{1}^{\infty} B_n$ where B_n is a direct sum of cyclic groups of order p^n. Then B is a basic subgroup of G if and only if $B_1 + \ldots + B_n$ is a maximal p^n-bounded direct summand of G for every integer n.

Proof: If B is a basic subgroup of G, then the group $G_n = \{B_n^*, p^n G\}$ has no nonzero direct summands of order $\leq p^n$. To see this, suppose that $\{c\}$ is a direct summand of G_n of order $p^r \leq p^n$; $p^{r-1}c \notin B$. By the divisibility of G/B we have $c = b + px$ for some $b \in B$ and $x \in G$. Now $b \in B_1 + \ldots + B_m$ for some m and $B_1 + \ldots + B_m + \{c\}$ is a direct summand of G. But then $px = c - b$ is impossible because, for some $x \in B_1 + B_2 + \ldots + B_m + \{c\}$, we have $x = mc - b_1$ ($b_1 \in B_1 + \ldots + B_m$, $mc \in c$, $m \neq 0$). Then $px = pmc - pb_1$, $c-b = pmc - pb_1$, $c(pm - 1) = pb_1 - b = 0$, by the direct summand property. But now $(pm - 1)$ must be some multiple of the order of $\{c\}$; i.e., $(pm - 1) = qp^r$ (q an integer) and this is impossible. To show that B is p^n-bounded, let $p^n x \in B$, then by the purity of B, $p^n x = p^n y$ for some $y \in B$. By the direct summand property, $y = b + b^*$ ($b \in B_1 + \ldots + B_n$, $b^* \in B_n^*$). Then $p^n y = p^n b + p^n b^* = 0 + p^n b^*$. We conclude $p^n x = p^n b^*$; i.e., $p^n x \in B_{n+1} + B_{n+2} + \ldots$.

Conversely, let $B = \sum B_n$ satisfy the stated condition. Then (i) and (ii) of the definition of basic sub-

groups are evident. In order to verify that G/B is divisible, we may argue as in the proof of Lemma 4.2. If the element c defined there had exponent $\leq n$, then $B_1 + \ldots + B_n + \{c\}$ would be a p^n-bounded pure subgroup; hence, a direct summand of G larger than $B_1 + \ldots + B_n$. Thus B is a basic subgroup.

We close this section with a remark. Consider G_n in (2). Any G_n has the property that $G_n[p]$ consists of all elements of G[p] which are of height $\geq n$. Since (2) implies $p^nG = p^nG_n$, the inclusion $(p^nG)[p] \subseteq G_n[p]$ is obvious. If $a \in G_n[p]$ were of height $r < n$, then we could imbed a in a direct summand of order p^{r+1} of G_n, contradicting Theorem 4.6.

Section 2

PROPERTIES OF BASIC SUBGROUPS

Each basic subgroup B of the p-group G gives rise to a generating system which plays a role similar to a basis. First, consider a basis $[a_\lambda]_{\lambda \in \Lambda}$ of B, $B = \Sigma \{a_\lambda\}$ and then write the factor group G/B as a direct sum of quasicyclic groups, $G/B = \sum_{\mu \in M} C_\mu^*$ where $C_\mu^* \cong \mathcal{C}(p^\infty)$. The group C_μ^* is generated by cosets $c_\mu^{(1)*}, \ldots, c_\mu^{(n)*}, \ldots \pmod B$ with $pc_\mu^{(1)*} = 0^*$, $pc_\mu^{(n+1)*} = c_\mu^{(n)*}$ for $n = 1, 2, \ldots$. Considering that B is pure, we can choose from each $c_\mu^{(n)*}$ an element $c_\mu^{(n)}$ of the same order p^n. Then we have

$$(4) \qquad pc_\mu^{(1)} = 0, \quad pc_\mu^{(n+1)} = c_\mu^{(n)} - b_\mu^{(n)} \text{ for } n \geq 1,$$

where $b_\mu^{(n)} \in B$. Since $c_\mu^{(n)}$ is of order p^n, $b_\mu^{(n)}$ is of order $\leq p^n$. The set of all $a_\lambda (\lambda \in \Lambda)$ and all $c_\mu^{(n)}$ $(\mu \in M)$, $n = 1, 2, \ldots$ is a generating system for G; it is called a quasibasis of G. This definition is motivated by the following result.

Theorem 4.6 Every element g of the p-group G may be written by means of a quasibasis $[a_\lambda, c_\mu^{(n)}]$ in the form

$$g = k_1 a_{\lambda_1} + \ldots + k_r a_{\lambda_r} + m_1 c_{\mu_1}^{(n_1)} + \ldots + m_s c_{\mu_s}^{(n_s)} \tag{5}$$

where the k_i and m_j are integers and no m_j is divisible by p. (5) is unique in the sense that g uniquely defines the terms $k_i a_{\lambda_i}$ and $m_j c_{\mu_j}^{(n_j)}$.

Proof: If $g \in G$, first represent the coset $g^* = g + B$ by means of $c_\mu^{(n)*}$ in the form $g^* = m_1 c_{\mu_1}^{(n_1)*} + \ldots + m_s c_{\mu_s}^{(n_s)*}$ where the m_j may be assumed not to be divisible by p. Hence, the terms $m_j c_{\mu_j}^{(n_j)*}$ and so $m_j c_{\mu_j}^{(n_j)}$ are uniquely determined by g^*. Next we put

$$g - m_1 c_{\mu_1}^{(n_1)} - \ldots - m_s c_{\mu_s}^{(n_s)} = k_1 a_{\lambda_1} + \ldots + k_r a_{\lambda_r}$$

where the terms $k_i a_{\lambda_i}$ are again uniquely determined since B is the direct sum of the $\{a_\lambda\}$ $(\lambda \in \Lambda)$.

The expression (5) is called the canonical form of g in terms of the quasibasis. We remark that $E(g) \geq \max(n_1, \ldots, n_s)$ in (5); in fact, this maximum equals $E(g^*)$.

We collect some important properties of basic subgroups. Let G be an arbitrary p-group and B one of its

basic subgroups.

A) By Theorem 4.4, $G = \{B, p^nG\}$ for each integer $n \geq 0$.

B) $B/p^nB \cong G/p^nG$ for each integer $n \geq 0$. By the purity of B and the first isomorphism theorem, we have

$$G/p^nG = \{B,p^nG\}/p^nG \cong B/(B \cap p^nG) = B/p^nB$$

because of the purity of B.

C) $p^nG/p^nB \cong G/B$ for every integer $n \geq 0$. By the purity of B and the first isomorphism theorem, we have

$p^nG/p^nB = p^nG/(B \cap p^nG) \cong \{B,p^nG\}/B = G/B$, by A).

D) $p^kG = \{p^kB, p^{n+k}G\}$ for all non-negative integers k and n. In fact, $p^kG = p^k\{B, p^nG\} = \{p^kB, p^{n+k}G\}$.

E) $p^nB/p^{n+1}B \cong p^nG/p^{n+1}G$ for each integer $n \neq 0$. Putting n = 1 in A) we have $G = \{B,pG\}$; then from D) and the first isomorphism theorem, we obtain $p^nG/p^{n+1}G = \{p^nB, p^{n+1}G\}/p^{n+1}G \cong p^nB/(p^nB \cap p^{n+1}G) = p^nB/p^{n+1}B$ because of the purity of B.

F) An upper bound may be given for the power (cardinal) of G in terms of a basic subgroup. If G is a reduced p-group and b is a basic subgroup of G, then $|G| \leq |B|^{\aleph_0}$. (For a proof, see Abelian Groups by Fuchs).[3]

G) If S is a pure subgroup of G, then G/B is divisible if and only if S contains a basic subgroup of G. To prove this, let G/B be divisible and B a basic subgroup of S. Then B is a direct sum of cyclic groups and is pure also in G by the transitive property of pure subgroups. Further, S/B is, as a divisible subgroup, a direct

summand of G/B, G/B = S/B + T/B. We know S/B is divisible by the definition of basic subgroups. By the second isomorphism theorem, T/B $\cong$ G/S, and, since S/B and T/B are divisible, G/B is also divisible, and we conclude that B is a basic subgroup of G. Conversely, if S contains a basic subgroup B of G, then G/B is a homomorphic image of G/B, and hence, it is divisible.

H) Theorem 4.8 Let G' be the subgroup of G consisting of all elements of G which are of infinite height and let $\overline{G} = G/G'$. Then the image $\overline{B}$ of a basic subgroup B of G under the natural homomorphism $G \to \overline{G}$ is a basic subgroup of $\overline{G}$, and $\overline{B} = B$.

Proof: Write $B = \Sigma B_n$ where B_n is a direct sum of cyclic groups of the same order p^n. By Theorem 4.4, we have $G = B_1 + \ldots + B_n + \{B_n^*, p^nG\}$ with $B_n^* = B_{n+1} + B_{n+2} + \ldots$. The relation $B \cap G' = 0$ shows that, under the natural homomorphism $G \to \overline{G}$, B is mapped isomorhically onto its image $\overline{B}$. Therefore $\overline{G} = \overline{B}_1 + \ldots + \overline{B}_n + \{\overline{B}_n^*, p^nG/G'\}$ where $p^nG/G8 = p^n\overline{G}$. By making use of Theorem 4.4 again, we are led to the desired conclusion.

I) A corollary to Theorem 4.8 asserts $|B| \leq |\overline{G}|$ for the group $\overline{G}$ defined there.

J) and F), together with I), imply

Corollary 4.9 For a reduced p-group G and for the group $\overline{G}$ defined in Theorem 4.8 we have $|G| \leq |\overline{G}|^{\aleph_0}$.

CHAPTER V

STRUCTURE RESULTS FOR p-GROUPS

Section 1

INTRODUCTION

Our first result refers to a p-group without elements of infinite height. Let $B = \sum_1^\infty B_n$ be a basic subgroup of an arbitrary p-group G where B_n is a direct sum of cyclic groups of the same order p^n. By the results of Section 1 of Chapter IV, we have $G = B_1 + B_2 + \ldots + B_m + G_m$ $(m = 1, 2, \ldots)$ where $G_m = \{B_{m+1} + B_{m+2} + \ldots, p^m G\}$. Any element $g \in G$ can be written in the form $g = b_1 + \ldots + b_m + g_m$ with $b_i \in B_i$ for $i = 1, 2, \ldots, m)$ and $g_m \in G_m$.

By definition, $G_m = B_{m+1} + G_{m+1}$, and it is clear that the elements b_i in the expression for g do not change if we pass from m to m + 1. We conclude that the b_i are uniquely determined, so that we can assign to each $g \in G$ an infinite sequence.

(1) $\qquad g \longrightarrow \langle b_1, \ldots, b_m, \ldots \rangle \qquad (b_m \in B_m).$

We observe that if $g' \longrightarrow \langle b_1', \ldots, b_m', \ldots \rangle$, then

$$g + g' \longrightarrow \langle b_1 + b_1', \ldots, b_m + b_m', \ldots \rangle$$

and so (1) gives rise to a homomorphism η of G onto a group V of sequences $\langle b_1, \ldots, b_m, \ldots \rangle$ with $b_m \in B_m$. It may be assumed that $B \subset V \subset \overline{B}$ where $\overline{B}$ is the maximal torsion subgroup of the complete direct sum of the

B_m (m = 1, 2, ...).

Theorem 5.1 Let G' be the subgroup of all elements of infinite height in a p-group G. Let $B = \sum_1^\infty B_n$ be a basic subgroup of G and let $\overline{B}$ be the maximal torsion subgroup of the complete direct sum $\sum_1^\infty * B_n$. Then G/G' is isomorphic to some pure subgroup V between B and $\overline{B}$.

Proof: If H(g) = ∞, then $g\eta = \langle 0, \ldots, 0, \ldots \rangle = \langle 0 \rangle$, because $g = b_1 + \ldots + b_m + g_m$ implies $H(g) = \min(H(b_1), \ldots, H(b_m), H(g_m))$. Then $H(b_i)$ cannot be finite and so $b_i = 0$. On the other hand, if H(g) is finite, $g\eta = \langle 0 \rangle$ as we will show by induction on the exponent of g. First let E(g) = 1, H(g) = n, then $g = b_1 + \ldots + b_{n+1} + g_{n+1}$ ($b_i \in B_i$, $g_{n+1} \in G_{n+1}$) shows that $b_1 = b_2 = \ldots = b_n = 0$ since $B_1, \ldots, B_n$ have no elements of height n. We conclude $g = b_{n+1} + g_{n+1}$ and $E(g_{n+1}) \leq 1$ follows by E(g) = 1; i.e., pg = 0, and the direct summand property by which $pg = 0 = pb_{n+1} + pg_{n+1}$ implies $pg_{n+1} = 0$. Further $H(g_{n+1}) \geq n + 1$, since by Theorem 4.5, G_{n+1} contains no cyclic direct summands of order $\leq p^{n+1}$. For example, if $H(g_{n+1})$ is exactly n, then $p^n x = g_{n+1}$ for some x in G_{n+1}. Then $p^{n+1}x = pg_{n+1} = 0$, so that x generates a subgroup of order p^{n+1}. We conclude $b_{n+1} \neq 0$. Next, let E(g) = k, H(g) = n, and suppose we have shown that no element of G of exponent $\leq k - 1$ and of finite height is mapped upon $\langle 0 \rangle$. If we had $g\eta = \langle 0 \rangle$, then also $(pg)\eta = \langle 0 \rangle$, and the induction hypothesis implies $H(pg) = \infty$, since

$E(pg) = k - 1$. Then there is $h \in G$ with $pg = p^{n+2}h$, and $g - p^{n+1}h$ is of exponent 1 and of height n. Consequently, $g - p^{n+1}h$ is mapped upon $\langle b_1, \ldots, b_n, \ldots \rangle$ such that $b_{n+1} \neq 0$. But the first $n + 1$ components of the sequence corresponding to $p^{n+1}h$ vanish since the height is $\geq n + 1$, and, therefore, $g\eta = \langle 0 \rangle$ is impossible. Thus, we have shown that the kernel of the homomorphism η: $G \longrightarrow B$ is G', the set of elements of infinite height in G. To verify that V is pure in $\overline{B}$, Theorem 4.8 states $B = \Sigma B_n$ is a basic subgroup of V and that V/B is divisible. Hence $z \in \overline{B}$ and $p^n z \in V$ imply the existence of some $x \in V$ with $p^n z - p^n x \in B$, and so for a suitable $b \in B$ we have $p^n(z - x) = p^n b$, because of the purity of B. In other words, $p^n z = p^n(x + b)$ where $x + b \in V$.

Corollary 5.2 If G is a p-group without elements of infinite height, then it is isomorphic to some pure subgroup of $\overline{B}$ containing B. (It will be convenient in this case to identify G with its image $G\eta$ in $\overline{B}$).

Section 2

CLOSED p-GROUPS

An investigation of one aspect of the groups $\overline{B}$ uses the notion of convergence and Cauchy sequences as they apply to groups. Let G be a p-group without elements of infinite height. A sequence $g_1, \ldots, g_n, \ldots$ of elements of G is said to converge to a limit g if $g - g_n \in p^n G$ for

$n = 1, 2, \ldots$. The limit g is unique since a second limit g' would satisfy $g' - g_n \in p^nG$, $g - g' \in p^nG$ for every n, so $g = g'$ because 0 is the only element common to all of the p^nG $(n = 1, 2, \ldots)$. If $g_n \to g$ and $g_n' \to g'$, then $g_n \pm g_n' \to g \pm g'$ and every subsequence of a convergent sequence is likewise convergent to the same limit. The sequence $g_1, \ldots, g_n, \ldots$ $(g_n \in G)$ is called a Cauchy sequence if the exponents of the elements g_n are bounded and for all n we have $g_n - g_{n+1} \in p^nG$. It follows that the sum and difference of two Cauchy sequences as well as a subsequence of a Cauchy sequence are again Cauchy sequences. A p-group without elements of infinite height is termed a closed p-group if every Cauchy sequence in G has a limit in G.

Theorem 5.3 A p-group G is closed if and only if $G = \overline{B}$ for some basic subgroup B of G.

Proof: Recall that if $B = \sum_1^\infty B_n$, $B_n = \sum \mathcal{C}(p^n)$, then $\overline{B}$ denotes the maximal torsion subgroup of the complete direct sum $\sum_1^\infty {}^*B_n$. Let $g_n = \langle b_1^n, \ldots, b_k^n, \ldots \rangle$ $(b_k^n \in B_k)$, $n = 1, 2, \ldots$ be a Cauchy sequence in $\overline{B}$; i.e., the exponents of the elements g_n are bounded and for all n we have $g_n - g_{n+1} \in p^nG$. Thus we have

$$g_1 = \langle b_1^1, b_2^1, \ldots, b_n^1, b_{n+1}^1, \ldots \rangle$$
$$g_2 = \langle b_1^2, b_2^2, \ldots, b_n^2, b_{n+1}^2, \ldots \rangle$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$g_n = \langle b_1^n, b_2^n, \ldots, b_n^n, b_{n+1}^{n+1}, \ldots \rangle$$

$$g_{n+1} = \langle b_1^{n+1}, b_2^{n+1}, \ldots, b_n^{n+1}, b_{n+1}^{n+1}, \ldots \rangle$$

. . . . . .

The inclusion relation

$$g_{n+1} - g_n = \langle b_1^{n+1}-b_1^n, \ldots, b_k^{n+1}-b_k^n, \ldots \rangle \varepsilon\, p^n\overline{B}$$

implies $b_1^{n+1}-b_1^n = \ldots = b_n^{n+1}-b_n^n = 0$; i.e., the first n components of g_n and g_{n+1} are identical. Further, $b_k^{n+1}-b_k^n \varepsilon\, p^nB_k$ for all k. Now the diagonal element $g = \langle b_1^1, b_2^2, \ldots, b_n^n, \ldots \rangle$ exists in $\overline{B}$ because $E(g_n)$ is bounded by hypothesis and so also $E(b_n^n)$ is bounded, and it satisfies $g - g_n = \langle 0, \ldots, 0, b_{n+1}^{n+1}-b_{n+1}^n, b_{n+2}^{n+2}-b_{n+2}^n, \ldots \rangle \varepsilon\, p^n\overline{B}$. This is equivalent to the assertion that g is the limit of the sequemce $g_1 \ldots, g_n, \ldots$. Thus $\overline{B}$ is closed. Next let G be a closed p-group and let $B = \Sigma B_n$ be a basic subgroup of G. By Corollary 5.2, G is isomorphic too and, therefore, may be regarded as identical with some group between B and $\overline{B}$, and, therefore, it is enough to show that each $\langle b_1, \ldots, b_n, \ldots \rangle \varepsilon\, \overline{B}$ represents an element of G. Since $\overline{B}$ is a maximal torsion subgroup; the exponents $E(b_n)$ are bounded. Let M = l.u.b. $E(b_i)$, $k_n > \max.(M,n)$, and $g_n = b_1 + \ldots + b_{k_n}$, where $k_n \geq n$, and k_n is such that $b_k \varepsilon\, p^nG$ for $k > k_n$. We then choose $k_n > M$. Then the $E(g_n)$ are bounded, and we have $g_{n+1} - g_n \varepsilon\, p^nG$; i.e., $g_1, \ldots, g_n, \ldots$ is a Cauchy sequence in G. Denote its limit by $g = \langle b_1', \ldots, b_n', \ldots \rangle$. Considering that $g-g_n = \langle b_1'-b_1, \ldots, b_{k_n}'-b_{k_n}, b_{k_n+1}, \ldots \rangle \varepsilon\, p^nG$, we

must have $b_1' - b_1 = \ldots = b_n' - b_n = 0$; i.e., $b_n' = b_n$ for every n. We are led to the conclusion that the arbitrarily chosen element of $\overline{B}$ is a limit of a Cauchy sequence in G (moreover in B); i.e., $G = \overline{B}$.

Corollary 5.4 Two closed p-groups are isomorphic if and only if their basic subgroups are isomorphic.

Proof: Note that any two basic subgroups of a p-group are isomorphic. On the other hand, if $B_1 \cong B_2$, then $\overline{B}_1 \cong \overline{B}_2$, and, therefore, Theorem 5.3 concludes the proof.

Section 3

THE ULM SEQUENCE

We here direct our attention toward p-groups having elements of infinite height and set as our goal the construction of a well-ordered sequence of p-groups without elements of infinite height which is a structural invariant.

Let G be an arbitrary p-group. We define subgoups G^α of G (where α is an ordinal) as follows: put $G^0 = G$ and assume we have already constructed every G^β for all $\beta < \alpha$. If $\alpha - 1$ exists, let G^α consist of all elements of $G^{\alpha-1}$ which are of infinite height in $G^{\alpha-1}$, while if α is a limit ordinal (for example, ω , the first infinite ordinal which has no immediate predecessor), then we define G^α as the intersection of all G^β with $\beta < \alpha$. Since the G^α form a descending chain of subgroups, there is certainly a least ordinal τ , not exceeding the cardinal of G, such that

$G^{\tau+1} = G^{\tau}$. Then $\tau = \tau(G)$ is said to be the Ulm Type of G. Since the equality $G^{\tau+1} = G^{\tau}$ means that every element of G^{τ} is of infinite height in G^{τ}, we see that G^{τ} is a divisible subgroup of G. Since divisible subgroups are direct summands, we may limit our attention to reduced groups G, and then G^{τ} must collapse to O.

The Ulm factors of G are defined to be the factor groups $G_\alpha = G^\alpha/G^{\alpha+1}$ for all $\alpha < \tau$. The well-ordered sequence $G_0, G_1, \ldots, G_\alpha, \ldots$ $(\alpha < \tau)$ is defined to be the Ulm sequence of G. We observe that the Ulm type, the Ulm sequence and the Ulm factors are uniquely determined by the reduced p-groups G. Clearly, $\tau(G) = 1$ if and only if G contains no elements of infinite height. As an example for the case $\tau(G) > 1$, let us consider the group generated by the elements $a_0, a_1, \ldots, a_n, \ldots$ subject to the defining relations $pa_0 = 0$, $a_0 = pa_1 = \ldots = p^n a_n = \ldots$. Then we have $G^1 = \{a_0\}$, $G^2 = 0$, and so G is of type 2 and its Ulm sequence is

$$G_0 = G/G^1 \cong \sum_1^\infty \mathcal{C}(p^n), \quad G_1 = G^1/G^2 \cong \mathcal{C}(p).$$

Lemma 5.5 Let η be a homomorphism of G onto H such that the kernel K contains only elements of infinite height. If $g\eta = h$ $(g \in G, h \in H)$, then $H(g) = H(h)$.

Proof: A homomorphism cannot diminish the height. To see this, suppose η is a homomorphism of the group G onto H, and $a\eta = a'$. Suppose $H(a) = n$; then for some $x \in G$, $p^n x = a$. Also let $x\eta = x'$, then $a\eta = a'$, $p^n x\eta = a'$, or

$p^n x' = a'$, and we conclude $H(a') \geq n$. Thus we have $H(g) \leq H(h)$. Conversely, if $p^n y = h$ in H, and x is some inverse image of y, then $p^n x = g + a$ $(a \in K)$. But $H(a) = \infty$; i.e., $p^z w = a$ is solvable for all integers z. In particular, there is a $v \in G$ such that $p^n v = a$. Then $(p^n x - p^n v) = g$, $p^n(x - v) = g$, with $(x - v) \in G$. We conclude $H(g) \geq H(h)$. Thus, we are led to the conclusion $H(g) = H(h)$ as desired.

In view of Lemma 5.5, we observe that no Ulm factor G_α contains elements of infinite height. In fact, every element of G^α outside $G^{\alpha+1}$ is mapped upon an element of the same finite height under the natural homomorphism $G^\alpha \to G^\alpha/G^{\alpha+1}$.

Lemma 5.6 All the Ulm factors G_α are unbounded p-groups with the possible exception of $G_{\tau-1}$, if this is non trivial.

Proof: Assume that $p^t G_\alpha = 0$ $(p^t(G^\alpha/G^{\alpha+1}) = 0)$ for some integer t and for some $\alpha < \tau$. Then $p^t G^\alpha \subseteq G^{\alpha+1}$ and every equation $px = a$ is solvable in G^α (for $a \in G^{\alpha+1}$ because it is of infinite height in G^α) and $p^t y = x \in G^{\alpha+1}$. We infer that $G^{\alpha+1}$ is divisible; then $G^{\alpha+1} = 0$ and only $\alpha + 1 = \tau$ is possible.

The Ulm sequence of G^β is $G_\beta, G_{\beta+1}, \ldots$. The initial part $G_0, \ldots, G_\alpha, \ldots$ $(\alpha < \beta)$ is also an Ulm sequence.

Lemma 5.7 The Ulm sequence of $H = G/G^\beta$ is $G_0, \ldots, G_\alpha, \ldots$ $(\alpha < \beta)$.

Proof: Since, by Lemma 5.5, the natural homomorphism

$G \to H$ preserves the height of the elements, we see that maps G^1 upon H^1; moreover, G^1 is the complete inverse image of H^1, for

$$G_1 = G^1/G^2 \cong (G^1/G^\beta)/(G^2/G^\beta) \cong H^1/H^2 = H_1.$$

We apply transfinite induction in order to show that G^α is the complete image of H^α under η. If $\alpha-1$ exists, then we may pass from $\alpha-1$ to α by the same inference as above from 0 to 1. If α is a limit ordinal, then the assertion follows from the definition of G^α and H^α, namely, $G^\alpha = \bigcap_{\nu<\alpha} G^\nu$ and $H^\alpha = \bigcap_{\nu<\alpha} H^\nu$. Since G^α is the complete inverse image of H^α we have the desired relationship between the G^ν and the H^ν. Now we have

$$G_\alpha = G^\alpha/G^{\alpha+1} \cong (G^\alpha/G^\beta)/(G^{\alpha+1}/G^\beta) \cong H^\alpha/H^{\alpha+1}$$
$$= H_\alpha \text{ as we wished to show.}$$

Lemma 5.8 Let $G = \sum_{\lambda \in \Lambda} G(\lambda)$ be a direct sum. Then for the Ulm factors G_α of G, we have $G_\alpha = \sum_{\lambda \in \Lambda} G_\alpha(\lambda)$ where the $G_\alpha(\lambda)$ are the Ulm factors of $G(\lambda)$ and we set $G_\alpha(\lambda) = 0$ whenever $\alpha \geq \tau(G(\lambda))$.

Proof: We first establish that $G^\alpha = \sum_{\lambda \in \Lambda} G^\alpha(\lambda)$. Assume that this has been proved for $\beta < \alpha$. If $\alpha-1$ exists, then $G^{\alpha-1} = \sum_{\lambda \in \Lambda} G^{\alpha-1}(\lambda)$ and so every element of $G^\alpha(\lambda)$ is of infinite height in $G^{\alpha-1}$; i.e., $G^\alpha \supseteq G^\alpha(\lambda)$ and $G^\alpha \supseteq \sum_{\lambda \in \Lambda} G^\alpha(\lambda)$. On the other hand, if $g \in G^{\alpha-1}$ is of infinite height, then $g = g_{\lambda_1} + \ldots + g_{\lambda_k}$ $(g_\lambda \in G^{\alpha-1}(\lambda))$ implies that each g_λ is of infinite height in $G^{\alpha-1}(\lambda)$; i.e.,

$g_{\lambda_i} \in G^{\alpha}(\lambda_i)$, and we are finished. If α -1 does not exist, then we form, according to the definition, the intersections and obtain $G^{\alpha} = \bigcap_{\lambda} G^{\alpha}(\lambda)$. Consequently, we conclude $G_{\alpha} = G^{\alpha}/G^{\alpha+1} \cong \Sigma^{\lambda} (G^{\alpha}(\lambda)/G^{\alpha+1}(\lambda)) = \sum_{\lambda} G_{\alpha}(\lambda)$.

Theorem 5.9 The Ulm sequence $G_{\alpha}(\alpha < \tau)$ of a reduced p-group G consists of p-groups without elements of infinite height and satisfies the following conditions:

$$\text{(i)} \quad \sum_{0 \leq \alpha < \tau} |G_{\alpha}| \leq |G| \leq \prod_{0 \leq \alpha < \min.(\omega, \tau)} |G_{\alpha}|,$$

where ω denotes the first infinite ordinal number;

$$\text{(ii)} \quad \sum_{\beta \leq \alpha < \tau} |G_{\alpha}| \leq |G_{\beta}|^{\aleph_0} \text{ for all } 0 \leq \beta < \tau;$$

$$\text{(iii)} \quad r(B_{\alpha+1}) \leq \text{fin } r(G_{\alpha}) \text{ for all } \alpha+1 < \tau,$$

where $B_{\alpha+1}$ is a basic subgroup of $G_{\alpha+1}$, and fin $r(G_{\alpha}) = \min_{n=0,1,\ldots} r(p^n G_{\alpha})$.

Proof: In (i), the first inequality holds because G is the union of all disjoint sets $G^{\alpha}-G^{\alpha+1}$ for $0 \leq \alpha < \tau$ where $G^{\alpha}-G^{\alpha+1}$ denotes the set of all elements of G^{α} which do not belong to $g^{\alpha+1}$, and clearly, $|G^{\alpha}-G^{\alpha+1}| \geq |G^{\alpha}/G^{\alpha+1}| = |G_{\alpha}|$. In order to establish the second inequality, we distinguish two cases. If τ is a positive integer, say n, then $|G| = |G/G^1||G^1/G^2|\ldots|G^n/G^{n+1}| = |G_o||G_1|\ldots|G_n|$. If $\tau \geq \omega$, then setting $\min_{k=0,1,\ldots} |G_k| = |G_s|$ we have $|G| = |G/G^s||G^s| = |G_o||G_1| \ldots |G_{s-1}||G^s|$. Applying Corollary 4.9 to the group G^s whose initial Ulm factor is G_s, we get $|G^s| \leq |G_s|^{\aleph_0} \leq |G_s||G_{s+1}|\ldots$ from which the

second inequality in (i) follows. We can verify (ii) at once, since for the group G^β we have

$$\sum_{\beta \leqq \alpha < \tau} |G_\alpha| \leqq |G^\beta| \leqq |G_=|^{\aleph_0}$$

by (i) and Corollary 4.9. To verify (iii), consider a basic subgroup $G_{\alpha+1} = \sum_{\lambda \in \Lambda} \{a_{\alpha+1,\lambda}\}$ of $G_{\alpha+1} \cong G^{\alpha+1}/G^{\alpha+2}$. By Lemma 5.7, $G_{\alpha+1}$ is an Ulm factor of $G^\alpha/G^{\alpha+2}$ and, therefore by definition for each positive integer n, the equation $p^n x_\lambda^{(n)} = a_{\alpha+1,\lambda}$ must have a solution $x_\lambda^{(n)}$ in $G^\alpha/G^{\alpha+2}$. We show that $\mu \neq \lambda$ implies $x_\mu^{(m)} \not\equiv x_\lambda^{(n)} \pmod{G_{\alpha+1}}$. Indeed, from $x_\lambda^{(n)} = x_\mu^{(m)} + a$ $(a \in G^{\alpha+1}/G^{\alpha+2} = G_{\alpha+1})$ it would follow (taking, say, $n \geqq m$) that

$$p^n a = p^n x_\lambda^{(n)} - p^n x_\mu^{(m)} = a_{\alpha+1,\lambda} - p^{n-m} a_{\alpha+1,\mu} \in B_{\alpha+1}.$$

Hence, by the purity of $B_{\alpha+1}$, we should get

$$a_{\alpha+1,\lambda} - p^{n-m} a_{\alpha+1,\mu} = p^n b \text{ for some } b \in B_{\alpha+1},$$

and this is impossible in the basic subgroup $B_{\alpha+1}$ because b can be written as a linear combination of the $a_{\alpha+1}$ which gives a relation where there is none. Taking into account that $x_\lambda^{(n)}$ is of order p^n modulo $G^{\alpha+1}$, we conclude that the set of elements of order p^n in G_α is of cardinal at least that of the set of the basic elements of $B_{\alpha+1}$. Thus, we arrive at the desired inequality.

We remark that as a result of (i) in Theorem 5.9, an upper estimate for the cardinal of a group G may be given if one knows nothing else than the first ω Ulm factors of G.

Section 4

ZIPPIN'S THEOREM

The results of this section and the next accomplish a complete classification of countable torsion groups. Recall that it suffices to do this for p-groups. For the remainder of this Chapter, we confine our attention to countable groups. If G is a countable reduced p-group, then its Ulm type is either finite or a countably infinite τ. The Ulm factors $G_\alpha (\alpha < \tau)$ of G are necessarily countable and the results of Section 3 of this Chapter imply that the G_α have no elements of infinite height. Applying the results of Theorem 1.9, we observe that every G_α is a direct sum of a countable set of cyclic groups of unbounded order with the possible exception of the last factor $G_{\tau-1}$ which might be bounded if it is non-trivial. Thus, for countable p-groups, the Ulm sequence is of a very simple nature.

Lemma 5.10 For a given group G, suppose that the set of subgroups $G_o = G^o, G^1, \ldots, G^{\tau-1}, G^\tau = 0$ has been formed in accordance with the description presented in the previous section. Further, suppose that the Ulm sequence for G is $G_o = G/G^1, G_1 = G^1/G^2, \ldots, G_{\tau-2} = G^{\tau-2}/G^{\tau-1}, G_{\tau-1} = G^{\tau-1}/K$ where K is a subgroup containing only elements of infinite height. Then division of each member of the set $G^o, \ldots, G^{\tau-1}$ by K does not alter the Ulm sequence $G_o, \ldots, G_{\tau-2}$.

Proof: Consider the factor groups G/K and G^1/K. We first show that if $x + K$ ($x \in G$) is of infinite height in G/K, then $x + K \in G^1/K$. Since $x + k$ is of infinite height, $x + K = p^n y + k$ for all n. Thus $x = p^n y - k$ ($k \in K$) and, because the elements of K are of infinite height, we have $k = p^n k_1$ ($k_1 \in G^1$). We conclude $x = p^n(y + k_1)$ and $x + K \in G^1/K$. On the other hand, if $x + K \in G^1/K$, then it is of infinite height in G/K. To see this, observe that $x = p^n y$ for some $y \in G$ since $x \in G^1$ because it is of infinite height in G. Therefore, $x + k = p^n y + k = p^n(y + K)$ for all n. We may now repeat this procedure for the pairs G^1/K and G^2/K, G^2/K and G^3/K, and so on, as desired.

Zippin's theorem states that if we are given a well-ordered countable sequence of countable groups $G_\alpha(\alpha < \tau)$ which are direct sums of cyclic groups of unbounded order, then there is a countable group G whose Ulm sequence is just $G_\alpha(\alpha < \tau)$.

Theorem 5.11 (Zippin) There is a countable reduced p-group G of type τ and with the Ulm sequence $G_\alpha(0 \leq \alpha < \tau)$ if and only if (i) τ is a finite or countably infinite ordinal, (ii) the groups $G_\alpha(0 \leq \alpha < \tau)$ are countable p-groups without elements of infinite height such that no G_α with $\alpha + 1 < \tau$ is bounded.

Proof: By Theorem 5.9 and Lemma 5.6, it is enough to prove the "if" part of the theorem. The proof is based on a transfinite induction with respect to τ. If $\tau = 1$,

then there is only one Ulm factor G_0, and $G = G_0$ is a group with the desired properties. Now we make the induction hypothesis that $\tau \geq 2$ and that the theorem holds for Ulm types less than τ. Five cases are distinguished and treated separately.

Case I: $\tau - 2$ exists and $G_{\tau-1}$ is a cyclic group, $G_{\tau-1} = \{a\} = \mathcal{C}(p^n)$. By Theorem 1.9, $G_{\tau-2}$ is a direct sum of cyclic groups, $G_{\tau-2} = \sum_1^\infty \{b_i\}$ where $E(b_i) = n_i \geq 0$. Define $\overline{G}_{\tau-2}$ by enlarging the exponents by n, i.e., $\overline{G}_{\tau-2} = \sum_1^\infty \{x_i\}$ with $E(x_i) = n_i + n$. By the induction hypothesis, there is a group H with the Ulm sequence $G_0, \ldots, G_\alpha, \ldots, \overline{G}_{\tau-2}$. Define G as the factor group of H with respect to the subgroup generated by the elements $p^{n_i}x_i - p^{n_j}x_j$ $(i,j = 1, 2, \ldots)$. Recalling that the exponents n_i are unbounded, we put $p^{n_i}x_i = a$, and apply Lemma 5.10, then the factor group $G/\{a\}$ is a group with the Ulm sequence $G_0, \ldots, G_\alpha, \ldots, G_{\tau-2}$. Since the elements x_i belong to $G^{\tau-2}$, we see that $a \in G^{\tau-1}$ and G is of type τ. To show that a is of order p^n, we map G homomorphically into a quasicyclic group Q in the following way. We send a upon an element of order p^n and then determine the image of x_i, recalling that $p^{n_i}x_i = a$. But the images of the x_i's induce a well-defined homomorphism of $\overline{G}_{\tau-2}$ onto Q, and as $\overline{G}_{\tau-2} \cong H^{\tau-2}$ is a subgroup of H, by Theorem 2.1 this homomorphism can be extended to a

homomorphism η of the whole of H onto Q. Under , $p^{n_k}x_i - p^{n_j}x_j$ is mapped upon O, so that η induces a homomorphism $G \to Q$ mapping a upon an element of order p^n, i.e., $O(a) = p^n$.

Case II: $\tau - 2$ exists and $G_{\tau-1}$ is a direct sum of cyclic groups, $G_{\tau-1} = \sum_1^\infty \{a_i\}$. In this case we decompose every G_α $(\alpha < \tau - 1)$ into an infinite direct sum of the subgroups $G_{\alpha i}$, $G_\alpha = \sum_1^\infty G_{\alpha o}$, such that no $G_{\alpha i}$ is bounded (here we use the unboundedness hypothesis). By Case I, for every i there is a reduced countable p-group G_i with Ulm sequence $G_{01}, \ldots, G_{\alpha i}, \ldots, G_{\tau-2,i}, \{a\}$. By Lemma 5.8, we conclude that $G = \sum_1^\infty G_i$ possesses the Ulm sequence G_α $(\alpha < \tau)$. (If $G_{\tau-1}$ is a finite group, similar inference applies).

Case III: $\tau - 1$ is a limit ordinal and $G_{\tau-1}$ is a cyclic group, $G_{\tau-1} = \{a\} \cong \mathcal{C}(p^n)$. Select a sequence τ_i of ordinals tending to $\tau - 1$ and decompose each $G_\alpha(\alpha < \tau - 1)$ into $G_\alpha = \sum_1^\infty G_{\alpha i}$ such that $G_{\alpha i} = O$ if $\alpha < \tau_i$, $G_{\tau_i i}$ is a cyclic group $\{b_i\}$, say, of order p^{n_i}, and all other $G_{\alpha i}$ are unbounded. There is no restriction in assuming that the $\{b_i\}$ are so chosen that for every $G < \tau - 1$ and for every integer m there is an i with $\tau_i < \sigma$ and $n_i > m$. Putting $\overline{G}_{\tau_i i} = \{x_i\}$ of order p^{n_1+n}, the induction hypothesis guaranteed the existence of countable reduced p-groups H_i of type $\tau_i + 1$ and with

the Ulm sequence $G_{01}, \ldots, G_{\alpha i}, \ldots, \overline{G}_{i} i$. Let $H = \sum_{1}^{\infty} H_i$ and define G as the factor group of H with respect to the subgroup generated by $p^{n_i}x_i - p^{n_j}x_j$ $(i,j = 1, 2, \ldots)$. By Lemma 5.7, $G/\{a\}$, $(a = p^{n_i}x_i)$ has the Ulm sequence $G_0, \ldots, G_\alpha, \ldots, (\alpha < \tau - 1)$ and $a \varepsilon G^{\tau-1}$. That a is actually of order p^n can be shown in the same manner as in Case I.

Case IV: $\tau - 1$ is a limit ordinal and $G_{\tau-1}$ is a direct sum of cyclic groups. The Case III method is modified as the Case I method was modified to treat Case II.

Case V: τ is a limit ordinal. We represent each $G_\alpha (\alpha < \tau)$ in the form $G_\alpha = G_{\alpha\alpha} + \ldots + G_{\alpha\sigma} + \ldots$ $(\alpha \leq \sigma < \tau)$ and suppose that every $G_{\alpha\sigma}$ is chosen so as to be unbounded. By the induction hypothesis, there is a countable reduced p-group H_α with the Ulm sequence $G_{0\alpha}, \ldots, G_{\alpha\alpha}$ for each $\alpha < \tau$. Then by Lemma 5.8, the group $G = \sum_{\alpha<\tau} H_\alpha$ has the indicated Ulm sequence.

Section 5

ULM'S THEOREM

The culminating result of our study asserts that two countable reduced p-groups are isomorphic if they have the same Ulm sequence. As a first step, we introduce a generalization of the concept of height which constitutes a refinement of the concept of infinite height. Suppose that G is a reduced p-group with the sequence $G^0, G^1, \ldots,$

$G^{\tau} = 0$ of subgroups formed as described in Section 3 of this chapter. Each nonzero element $a \in G$ determines a first ordinal β such that $a \notin G^{\beta}$. This β is not a limit ordinal because if $a \in G^{\alpha}$ for all α less than a limit ordinal β, then also $a \in G\, G^{\beta}$. Thus, β may be written in the form $\beta = \delta + 1$. Since $a \in G^{\delta}$ but $a \notin G^{\delta+1}$, we conclude that a is of finite height n in G^{δ}. The pair (δ,n) will be assigned to the element a as its <u>generalized height in G</u>. Unless otherwise stated, the symbol $H(a)$ will be used to denote the generalized height of a for the remainder of this chapter, i.e., $H(a) = (\delta,n)$. We define $H(0) = (\tau,0)$. The heights can be linearly ordered lexicographically by agreeing to put $(\delta,n) > (\delta',n')$ when either $\delta > \delta'$ or $\delta = \delta'$ and $n > n'$. The fundamental inequalities concerning height survive in this refined context

(1) $H(x) < H(y)$ implies $H(x + y) = H(x)$;

(2) $H(x) = H(y)$ implies $H(x + y) \geq H(x)$, since $<$ would contradict (1).

We also make use of a third inequality

(3) If $x \neq 0$, then $H(px) > H(x)$.

Suppose that U is a subgroup of the group G and V is a subgroup of the group H and that φ is an isomorphism between U and V. Then φ is called <u>height-preserving</u> if $H(u\varphi) = H(u)$ for all $u \in U$. Every isomorphism between G and H is height-preserving.

Let U be a subgroup of G and x an element of G which is not in U. We call x proper with respect to U if $H(x) \geq H(x + u)$ for all $u \in U$, i.e., x is of maximal height in its coset modulo U. If U is a finite group, then a proper x exists in every coset modulo U. We observe that if x is proper with respect to U, then $H(x + u) = \min (H(x), H(u))$ for all $u \in U$.

Lemma 5.12 Let G and H be two countable reduced p-groups with the same Ulm sequence and let φ be a height-preserving isomorphism of a finite subgroup U of G onto a subgroup V of H. If $b \in G$ and $b \notin U$, then there is a finite subgroup $\overline{U}$ of G and a subgroup $\overline{V}$ of H such that $\overline{U}$ contains U and b, and there is a height-preserving isomorphism Ψ mapping $\overline{U}$ onto $\overline{V}$ and agreeing in U with φ.

Proof: There will be no loss of generality in assuming $pb \in U$, for if $p^k b \in U$, $k > 1$, then the adjunction of b to U may be carried out be successive adjunctions of $p^{k-1}b, \ldots, pb, b$. Assume the hypothesis of the lemma, and let $pb \in U$. The coset $b + U$ contains elements proper with respect to U, since U is finite. If b' is such an element, then $pb' \in U$ and among the finitely many b' there is one, a, with maximal H(pa). We prove the existence of an element $c \in H$ which is proper with respect to V and satisfies $H(c) = H(a) = (\delta, n)$, $pc = (pa)\varphi$. Two cases are distinguished.

Case I: $H(pa) = (\delta, n+1)$. By virtue of the

hypothesis on φ , $(pa)\varphi$ has the height $(\delta,n+1)$, and therefore there is some $c \in H$ such that $pc = (pa)\varphi$, $H(c) = (\delta,n)$. Now $c \notin V$ for if $c \in V$ then we could find an element $u \in U$ with $u\varphi = c$; then $(pa)\varphi = (pu)\varphi$, $pa = pu$, $p(a-u) = 0$, where $a-u \notin U$. Since a is proper with respect to U, we have $H(a-u) = \min (H(a),H(u)) = (\delta,n)$, and a-u is likewise proper with respect to U. But $H(pa) = (\delta,n+1) < H(p(a-u)) = H(0)$ is in contradiction to the maximal choice of $H(pa)$. Further, c is proper with respect to V. If not, there is an element $v \in B$ such that $H(c+v) > H(c)$. Putting $v\varphi^{-1} = u \in U$, we have $(\delta,n) = H(c) < H(c+v) < H(pc+pv) = H(pa+pu)$, from which we obtain $H(p(a+u)) \geqq (\delta,n+2)$, again a contradiction to the same fact.

Case II: $H(pa) > (\delta,n+1)$. Then there is an element $a' \in G$ such that $pa' = pa$ and $H(a') \geqq (\delta,n+1)$. Hence $H(a-a') = H(a) = (\delta,n)$. Further, $a-a' = a''$ is again proper with respect to U, as seen by considering the following: by the maximality of $H(a)$ we have $H(a+u) \leqq H(a)$. Then we have $H(a+u) < H(a')$. By property (1), we have $H(a+u-a') = \min (H(a+u),H(a')) = H(a+u) \leqq H(a) = H(a--a')$, again by property (1). We now make use of the isomorphism of the Ulm sequences of G and H. Write $P_{\alpha n}$ for the socle of p^nG^α and $Q_{\alpha n}$ for the socle of p^nH^α. Since the rank $r(P_{\alpha n}/P_{\alpha,n+1})$ is equal to the number of the cyclic direct summands of order p^{n+1} in G_α, we get $r(P_{\alpha n}/P_{\alpha,n+1}) = r(Q_{\alpha n}/Q_{\alpha,n+1})$. Now φ carries $U_{\alpha n} = U \cap p^nG^\alpha$ into $V_{\alpha n} =$

$V \cap p_n H^\alpha$, and $U'_{\alpha n}$ into $V'_{\alpha n}$ where $U'_{\alpha n}$ is the subgroup of all $u \in U_{\alpha n}$ with $H(pu) \geq (\alpha, n+2)$. Then $U_{\alpha n} \supseteq U_{\alpha,n+1}$ and $V_{\alpha n} \supseteq V'_{\alpha n} \supseteq V_{\alpha,n+1}$. Further, $r(U'_{\alpha n}/U_{\alpha,n+1}) = r(V'_{\alpha n}/V_{\alpha,n+1})$ because φ is height preserving. The definition of $U'_{\alpha n}$ implies that to any $u \in U'_{\alpha n}$ there exists an element $y \in p^{n+1}G^\alpha$ such that $pu = py$. Hence $z = u-y$ satisfies $z \in P_{\alpha n}$, and another choice of y leads to the same z modulo $P_{\alpha,n+1}$. Therefore $u \to z + P_{\alpha,n+1}$ is a homomorphism of $U'_{\alpha n}$ onto a subgroup P^*_α of $P_{\alpha n}/P_{\alpha,n+1}$, the kernel of which is $U_{\alpha,n+1}$. Thus $U'_{\alpha n}/U_{\alpha,n+1}$ is isomorphic to the subgroup p^*_α of $P_{\alpha n}/P_{\alpha,n+1}$. The coset $a'' + P_{\delta,n+1}$ does not belong to P^*_δ, for otherwise there would exist an element $u \in U'_{\delta n}$ with $a'' - u \in p^{n+1}G^\delta$, $H(a''-u) > H(a'')$, contradicting the fact that a'' is proper with respect to U. This shows that $r(U'_{\delta n}/U_{\delta,n+1}) = r(P^*_\delta)$ is smaller than $r(P_{\delta n}/P_{\delta,n+1})$, and so $r(V'_{\delta n}/V_{\delta,n+1})$ is smaller than $r(Q_{\delta n}/Q_{\delta,n+1})$. If we define Q^*_α in $Q_{\alpha n}/Q_{\alpha,n+1}$ analogously, then it follows that $Q_{\delta n}/Q_{\delta,n+1}$ contains elements outside Q^*_δ. If $c' \in Q_{\delta n}$ is such an element, then it must be proper with respect to V. For if not, then $H(c'-v) > H(c')$ for some $v \in V$. Hence $H(v) = (\delta, n)$ and $c' - v = pt$ for some $t \in p^n H^\delta$. Multiplying p we obtain $0 - pv = p^2 t$, whence $H(pv) \geq (\delta, n+2)$ and $v \in V'_{\delta n}$. But then $c' + Q_{\delta,n+1} \in Q^*_\delta$ would be a contradiction. To see this, take a $v \in V'_{\alpha n}$, and find a $y \in p^{n+1}H^\delta$ such that $pv = py$. From $p(c'-v) = pc'-pv = -pv$

we have $-(c'-v) \in p^{n+1}H^{\delta}$ and $v \to v+(c'-v) = c'$. Since $H(pa) > (\delta,n+1)$, there exists $d \in H$ with $H(d) \geq (\delta,n+1)$ and $pd = (pa)\varphi$. Putting $c = c' + d$, then $H(c) = H(c') = (\delta,n)$, $pc = pc' + pd = (pa)\varphi$, and c is proper with respect to V. We conclude that in both cases there is an element $c \in H$ with the desired properties. Now we may extend φ to an isomorphism Ψ of $\{U,b\} = \{U,a\}$ onto $\{V,c\}$ by sending a upon c. Then Ψ is again height-preserving since $H(a+u) = \min(H(a),H(u)) = \min(H(c),H(v)) = H(c+v)$ whenever $u \in U$, $v \in V$ and $u\varphi = v$. This completes the proof of the lemma.

Theorem 5.13 (ULM) Two countable reduced p-groups G and H are isomorphic if and only if they have the same Ulm type τ and for each ordinal α $(0 \leq \alpha < \tau)$, the Ulm factors G_α and H_α are isomorphic.

Proof: In the proof we have to make certain that our construction yields an isomorphism between all of G and all of H. To do this, we number off, once for all, the elements of G and H. Then at the (2n-1)-th step, we look after the n-th element of G; at the 2n-th step, we look at the n-th element of H. This alternation between G and H is an indispensable divice. If for instance, we confine our attention to G, it is possible that we could end up with an isomorphism between G and part of H.

Since both G and H are countable reduced p-groups, we may arrange their elements in sequences (of type ω): $G = [g_1, g_2, \ldots]$, and $H = [h_1, h_2, \ldots]$. We put

$U_0 = V_0 = 0$, and assume the existence of a height-preserving isomorphism φ has been established between some finite subgroup U_n of G and V_n of H. If n is even, take the first g_k not in U_n and extend φ_n, by Lemma 5.12, to a height-preserving isomorphism φ_{n+1} of U_{n+1} onto V_{n+1}, where U_{n+1} is some subgroup of G including U_n and g_k, while V_{n+1} is a suitable subgroup of H (containing V_n). If n is odd, take the first h_j not in V_n and do the same with the inverse φ_n^{-1}. Because of this alternation between G and H, every element of G and H takes its turn and finally we arrive at a height-preserving isomorphism between G and H.

Section 6

CONCLUSION

We justify the choice of Theorems 1.9, 5.11, and 5.13 as the most far reaching results encountered in our discussion. These three results enable us to classify completely all countable reduced p-groups by means of invariants.

We begin by considering a countable reduced p-group G and a corresponding matrix M(G),

$$\begin{bmatrix} n_{01} & n_{02} & n_{03} \cdots & n_{0k} \cdots \\ \cdots & \cdots & \cdots & \cdots \\ n_{\alpha 1} & n_{\alpha 2} & n_{\alpha 3} \cdots & n_{\alpha k} \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

with a countable number of rows and a countable number of columns. The correspondence is accomplished as follows. The rows are arranged according to the type τ of G and the columns are arranged in a sequence of type ω. In the row of index α ($0 \leq \alpha < \tau$) the k-th element $n_{\alpha k}$ is a non-negative integer or the symbol ∞, and represents the number of cyclic direct summands of order p^k in a direct decomposition of the Ulm factor G_α of G. Each row has infinitely many nonzero entries with the possible exception of the τ-1 st row if it exists at all. Now the three mentioned theorems imply that this correspondence between the countable reduced p-groups and the matrices of the mentioned type is one-to-one. Hence these matrices can be considered as complete systems of invariants for countable reduced p-groups.

As a final remark, we recall that in the proof of Zippin's Theorem we had need of the results of Theorem 2.1. In particular, the theorem states that for a subgroup H of the group G, any homomorphism of H into a divisible group D can be extended to a homomorphism of the entire group G into D.

Theorem 5.14 If H is a countable reduced p-group, any automorphism of H^α can be extended to an automorphism of H, where α is any ordinal not greater than τ.

For the proof of the last statement, the reader is referred to an article in the Annals of Mathematics,

Section 2, (1935), Vol. 36, page 86 - 99 written by Leo Zippin and entitled Countable Torsion Groups.

The proof closely parallels the proof employed in the proof of Ulm'e Theorem. In addition the present theorem is stronger than the results of Theorem 2.1.

LIST OF REFERENCES

1. Baer, R., The decomposition of Abelian Groups into Direct Summands, Quart. J. of Math. 6, 217-221 (1935)

2. Chevalley, c., Fundamental Concepts of Algebra, Academic Press, 1956.

3. Fuchs, L., Abelian Groups, Pergamon Press, 1960.

4. Hall, M., The Theory of Groups, Macmillan, 1959.

5. Jacobson, N., Lectures in Abstract Algebra, D. Van Nostrand, 1951.

6. Kaplansky, I., Infinite Abelian Groups, University of Michigan Press, 1954.

7. van der Waerden, B. L., Modern Algebra, Revised English Edition, Frederick Ungar Publishing Co., 1953.

8. Zariski, S., 2nd Samuel, P., Commutative Algebra Vol. I, D. Van Nostrand, 1958.

9. Zippin, L., Countable Torsion Groups, Annals of Math., 36(1935), 86-99.